Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Deep Learning Models for Intrusion Detection Using a Text-to-Image Representation Approach

[1]Winit N. Anandpwar, [2]Shweta M. Barhate, [3]Mahendra P. Dhore
[1]Research Scholar, Dr. Ambedkar College, Nagpur, RTM Nagpur University, Nagpur, Maharashtra
winit.anand@gmail.com
ORCID iD: 0009-0001-5758-2190
[2]Associate Professor, Department of Electronics and Computer Science, PGTD, R.T.M. Nagpur University Nagpur Maharashtra India
shwetab73@yahoo.com
[3]Professor & Pro-Vice Chancellor, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India
mpdhore@rediffmail.com

ARTICLE INFO

Received: 22 Oct 2024
Revised: 24 Nov 2024
Accepted: 12 Dec 2024

ABSTRACT

Intrusion Detection Systems (IDS) play a critical role in safeguarding modern digital infrastructures, especially in automotive and IoT environments where cyber threats are increasingly prevalent. Traditional IDS methods often struggle with limited adaptability, high false alarm rates, and performance inefficiencies in real-time, resource-constrained settings. To address these challenges, this paper proposes a novel intrusion detection framework that integrates text-to-image conversion of CAN (Controller Area Network) traffic data with deep learning models. The structured textual dataset is transformed into 9×9×3 RGB image representations, enabling the application of advanced CNN-based models such as EfficientNetB0 and InceptionV3. These models are selected for their computational efficiency and high classification accuracy. Experiments conducted on the OCSLab Car-Hacking Dataset demonstrate that the proposed approach significantly outperforms traditional machine learning models in terms of accuracy, F1 score, and computational efficiency. This framework presents a scalable and real-time solution for intelligent and secure vehicular systems.

Keywords: Intrusion Detection System (IDS), Text-to-Image Conversion, Lightweight Deep Learning, EfficientNetB0, InceptionV3, Automotive Cybersecurity, CAN Bus, Transfer Learning, SMOTE, Vehicle Network Security.

1. Introduction

In the contemporary era of digital transformation, cybersecurity has become an indispensable component of modern computing environments, particularly with the exponential rise in the number of connected devices and the growing complexity of digital systems. Among the numerous domains affected by cyber threats, the automotive sector has recently emerged as a critical target due to the proliferation of connected vehicles and the integration of advanced electronic control units (ECUs) communicating via Controller Area Networks (CAN). Intrusion Detection Systems (IDS) have thus evolved as essential tools to monitor and detect malicious behavior in these environments [1]. However, traditional IDS methods are often limited by high computational overheads, inability to generalize across varied data distributions, and poor adaptability to real-time constraints — especially in embedded and resource-constrained scenarios like smart vehicles. To address these challenges, researchers have increasingly turned to deep learning (DL) approaches [2], which offer high adaptability, scalability, and robustness in identifying patterns within large and complex datasets. Conventional deep learning models such as Convolutional Neural Networks (CNNs) [3] and Recurrent Neural Networks (RNNs) [4] have demonstrated significant success in intrusion detection across several domains. However, these models often demand substantial computational resources, making them unsuitable for deployment in low-power and embedded environments. Consequently, there is a growing interest in developing deep learning architectures that provide high accuracy while maintaining computational efficiency.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

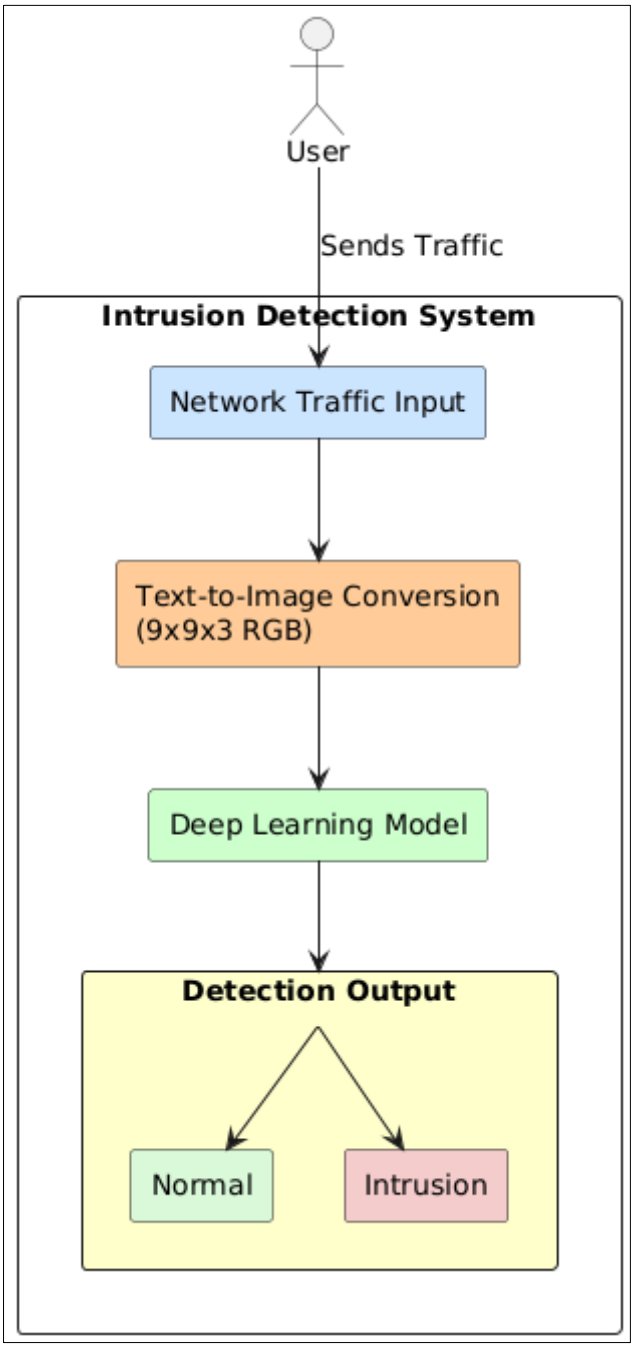

Figure 1. Overview of Intrusion Detection System

One of the innovative directions explored in this paper is the conversion of textual IDS data into image formats, a technique that leverages the powerful feature extraction capabilities of computer vision models for cyber threat detection. This transformation aligns with the broader trend in deep learning research that seeks to reinterpret non-image data (e.g., tabular, textual, or time-series data) as visual representations. By converting structured network traffic data into RGB images, we enable the application of image-based deep learning models — particularly lightweight transfer learning models — to the IDS domain [5][6]. This paper proposes a novel framework that integrates text-to-image data transformation with lightweight deep learning models such as EfficientNetB0 and InceptionV3. These models have been specifically selected for their architectural efficiency and high accuracy despite

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

reduced parameter counts, which makes them ideal for real-time intrusion detection in automotive and IoT systems. The central idea is to reshape a sequence of CAN data packets into a visual format (RGB images), allowing the models to learn spatial correlations between features that are not immediately obvious in raw text or numerical formats [7].

To achieve this, the OCSLab Car-Hacking Dataset — a publicly available benchmark dataset capturing real-world vehicle CAN bus traffic under normal and attack scenarios — is utilized. The dataset contains both benign and malicious messages representing various cyber-attacks, including spoofing, denial of service (DoS) [8], and fuzzy attacks. Preprocessing steps include handling missing values, normalizing feature ranges using standard scaling, and applying Synthetic Minority Oversampling Technique (SMOTE) [9] to resolve class imbalance. Following this, every 27 rows of the structured data are transformed into 9x9x3 RGB images using the PIL.Image module. This novel representation captures not just feature-wise but also temporal patterns across consecutive samples. The significance of this research lies in its ability to bridge the gap between high-performance IDS and real-world deployment constraints. By converting textual features to images, we not only enhance the model's pattern recognition capabilities but also unlock the potential to apply state-of-the-art image classification techniques to cybersecurity. Furthermore, the use of lightweight models ensures low latency and low power consumption, making the system suitable for embedded environments such as ECUs in vehicles, IoT edge nodes, or other safety-critical infrastructure.

Another noteworthy aspect of this research is its contribution to data representation engineering — the act of transforming raw or structured data into formats that are more conducive for deep learning. While the cybersecurity community has historically focused on packet-level or flow-level numerical analysis, this work takes inspiration from the fields of computer vision and multimodal learning to introduce a visually interpretable representation. This not only improves detection accuracy but also opens new avenues for explainable AI, where visualizations can be used to interpret model decisions. This framework is highly adaptable and can be extended to other datasets and domains beyond automotive IDS. The principles of text-to-image conversion, model selection based on deployment constraints, and performance evaluation metrics like confusion matrix, precision, recall, and F1-score provide a generalized methodology for any intrusion detection scenario. Furthermore, due to the modular design of the framework, it is possible to integrate additional components such as autoencoders for anomaly detection, attention mechanisms for interpretability, or federated learning for privacy preservation.

This paper addresses a critical challenge in modern IDS — achieving a balance between detection performance and computational efficiency — through a unique fusion of data transformation and deep learning. By transforming structured IDS data into images and applying lightweight CNN-based transfer learning models, we demonstrate that high-performance intrusion detection is not only possible but also practical for real-world constrained environments. The proposed approach lays the foundation for further research into cross-domain applications of visual deep learning models in security and for deploying resource-aware AI solutions in embedded and edge-based systems.

2. Literature Review

The field of Intrusion Detection Systems (IDS) has seen extensive research over the past two decades, evolving in response to the ever-growing sophistication of cyber threats across both enterprise networks and specialized domains like vehicular communication systems. Traditional IDS approaches are broadly categorized into signature-based and anomaly-based techniques [10]. Signature-based systems, like Snort and Bro, rely on predefined patterns to identify known attacks but are ineffective against zero-day vulnerabilities. Anomaly-based IDS, on the other hand, construct a profile of normal network behavior and raise alerts for any significant deviations. While this method shows promise for detecting novel attacks, it is plagued by high false-positive rates and a lack of interpretability. To address these limitations, researchers have increasingly explored Machine Learning (ML) and Deep Learning (DL) approaches, which offer data-driven adaptability and generalization capabilities beyond manual rule-based systems. In recent years, machine learning has played a central role in the development of data-driven IDS. Commonly used ML algorithms include Decision Trees (DT) [11], Support Vector Machines (SVM) [12], K-Nearest Neighbors (KNN) [13], and Random Forest (RF) [14]. These models leverage

statistical patterns within the data to classify normal and malicious behaviors. However, ML models often require manual feature engineering and lack the scalability needed for high-dimensional data or real-time detection in modern networks.

The shift towards deep learning was driven by the need for automatic feature extraction and hierarchical representation learning. DL architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have been effectively applied to detect cyber attacks in both traditional IT and specialized environments like the Internet of Things (IoT) and vehicular networks. For instance, a CNN-based intrusion detection model performed well on the NSL-KDD dataset, surpassing many conventional ML models [15]. A combined CNN-LSTM model leveraged the spatial feature extraction capabilities of CNNs and the sequential modeling strength of LSTMs to detect attacks with temporal patterns [16]. Despite their accuracy, such models are computationally expensive and not well-suited for deployment in embedded or low-power environments such as automotive ECUs. In response to deployment challenges, researchers have proposed lightweight neural network models that maintain high accuracy with fewer parameters and reduced inference time. Models such as MobileNet [17], SqueezeNet [18], EfficientNet, and InceptionV3 have been developed for mobile and embedded vision tasks but are now being repurposed for security applications. For instance, the EfficientNetB0 model utilizes a compound scaling method that uniformly scales depth, width, and resolution. This architecture achieves state-of-the-art performance on ImageNet with significantly fewer parameters than traditional models like ResNet or VGG. When applied to IDS tasks, these lightweight models show promise for balancing detection performance with resource constraints.

A parallel line of research focuses on data representation techniques that transform structured or sequential data into formats more conducive to DL models. One such approach is the conversion of tabular or textual data into image representations, which enables the application of powerful CNN architectures originally developed for computer vision tasks [19]. Researchers have also applied spectrogram-based transformations to time-series data in areas like finance and audio signal processing. In the context of IDS, such transformations are relatively new but growing in relevance. A deep learning model used encoded network traffic as grayscale images and fed them into a CNN for attack detection [20]. The visual encoding captures spatial correlations and interaction patterns between features, which might be overlooked by traditional numerical approaches. In the automotive domain, CAN bus security has emerged as a focal point due to the increasing number of attacks targeting vehicle communication protocols. The OCSLab Car-Hacking Dataset has been widely adopted for evaluating IDS performance in automotive settings [21]. LSTM-based IDS models have been developed using this dataset to model temporal dependencies in CAN messages. Entropy-based anomaly detection methods have also been used for identifying attacks in vehicle networks. However, these approaches often face issues such as high memory usage, slow inference, or an inability to adapt to dynamic threats.

To overcome these challenges, the integration of lightweight CNNs with visual encoding of textual data presents a compelling solution. This strategy not only leverages the high pattern recognition power of CNNs but also enables low-latency inference suitable for real-time vehicular IDS. Recent studies have demonstrated the effectiveness of image-based data transformation combined with MobileNet for detecting IoT-based malware [22]. Inspired by such innovations, the present research builds a pipeline that converts structured CAN traffic data into 9×9×3 RGB images and utilizes EfficientNetB0 and InceptionV3 to classify normal versus malicious behavior. The novelty lies in the transformation of automotive IDS data into image formats and the selection of lightweight models that offer superior performance under constrained computational budgets. This research is aligned with efforts in intrusion detection benchmarking. Several prior works have relied on outdated datasets such as KDD99 or NSL-KDD, which do not reflect modern cyber threats or realistic traffic patterns. The use of the OCSLab Car-Hacking Dataset, which includes realistic in-vehicle attacks, provides a more robust and applicable testing ground for IDS models. Additionally, performance evaluation in previous literature has often focused solely on accuracy, ignoring other crucial metrics like F1-score, confusion matrix, or computational cost. In contrast, this research adopts a comprehensive evaluation methodology that includes accuracy, F1-score, confusion matrix, and comparative analysis of model efficiency.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Another dimension of relevance in the literature is handling data imbalance, a common challenge in IDS datasets where attack samples are underrepresented compared to benign traffic. To tackle this, techniques such as Synthetic Minority Over-sampling Technique (SMOTE) have been employed. When combined with deep classifiers, SMOTE significantly improves model sensitivity toward rare attacks. In this research, SMOTE is used during the preprocessing phase to ensure a balanced training dataset, enabling the deep models to learn representative features from all classes. The literature reveals a strong shift from traditional rule-based and ML-based IDS towards deep learning methods. Yet, challenges such as computational cost, data representation, and model interpretability persist. The integration of lightweight CNNs with text-to-image data transformation addresses many of these limitations. It enables the application of mature vision-based architectures to structured intrusion data while ensuring compatibility with low-power deployment environments. Despite some progress in this area, the specific combination of text-to-image transformation and lightweight transfer learning for automotive IDS remains underexplored, marking a clear research gap that this study aims to fill.

3. Methodology

The proposed methodology shown in figure 2, aims to develop an efficient and accurate intrusion detection system (IDS) by transforming textual CAN data into image-based representations and leveraging lightweight deep learning models for classification. The framework is designed for real-time applications in resource-constrained environments, particularly in the automotive domain. This section elaborates on the step-by-step workflow including data acquisition, preprocessing, SMOTE balancing, image transformation, model selection, training, and evaluation.

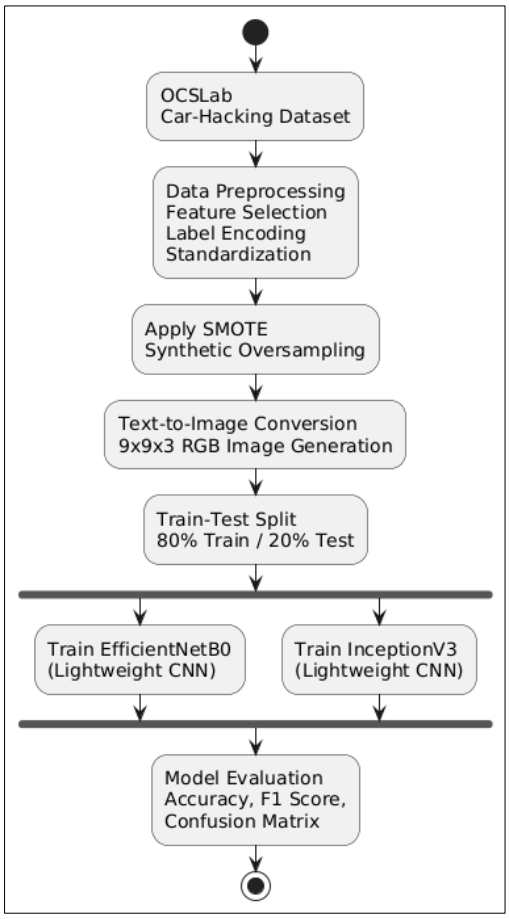

Figure 2. Proposed Methodology

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.1 Dataset

The study utilizes the **OCSLab Car-Hacking Dataset**, a publicly available benchmark dataset for vehicular cybersecurity research. The dataset consists of CAN (Controller Area Network) messages recorded under both normal and attack conditions, simulating real-world automotive cyber threats such as spoofing, denial of service (DoS), and fuzzy attacks. Each record contains various features such as timestamp, CAN ID, data length code (DLC), and eight bytes of hexadecimal data representing the message payload. The dataset is well-suited for classification tasks due to its clear labeling of benign and malicious samples.

3.2 Data Preprocessing

Effective data preprocessing is crucial to ensuring the quality and consistency of input for the deep learning pipeline. The following steps were carried out:

- **Feature Extraction and Label Encoding**: Relevant numerical features were selected from the dataset. Categorical variables were encoded using label encoding for target labels to convert them into a machine-readable format.
- **Handling Missing Values**: Any missing or corrupted entries were either removed or replaced with appropriate statistical values such as mean or median, depending on the distribution.
- **Standardization**: The feature values were standardized using **StandardScaler** to bring all features to a common scale (zero mean and unit variance), which helps in faster convergence during model training.

3.3 Class Imbalance Handling Using SMOTE

The dataset exhibited a significant imbalance between benign and attack samples, which could bias the learning process. To overcome this, the **Synthetic Minority Over-sampling Technique (SMOTE)** was applied. SMOTE works by generating synthetic examples in the feature space rather than duplicating existing minority class samples. This ensures a more robust learning process and mitigates the risk of overfitting. The balanced dataset post-SMOTE application includes equal representation from all classes, enhancing the sensitivity of the classifiers toward minority class attacks.

3.4 Text-to-Image Conversion

A core innovation in this methodology is the **transformation of textual data into image format** to leverage the spatial learning capabilities of CNN-based models. The process is as follows:

1. **Row Aggregation**: Each image is constructed using 27 consecutive rows from the dataset, which are reshaped into a 3D tensor (9×9×3), simulating an RGB image.
2. **Pixel Conversion**: Feature values were normalized to the 0–255 pixel range and converted to uint8 format to match image standards.
3. **Image Generation**: The reshaped tensors were converted into image objects using Python's PIL.Image.fromarray() function.
4. **Image Storage**: Generated images were saved in PNG format and organized into folders corresponding to their class labels (benign or attack).
5. **Looping Mechanism**: The conversion loop continued until the entire dataset was exhausted, ensuring each image captured sequential contextual information from the original dataset.

This transformation effectively allowed CNNs to exploit local and global correlations across sequential CAN messages, improving classification performance.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.5 Data Partitioning

The transformed image dataset was divided into training and testing sets using an 80:20 split ratio. This approach ensures that the models are trained on a large portion of the data while reserving a representative subset for unbiased evaluation.

3.6 Model Selection and Training

Two categories of models were employed:

A. Baseline Machine Learning Models

- **Logistic Regression (LR)**: A linear model used for binary classification tasks, serving as a baseline.
- **Stochastic Gradient Descent (SGD)**: An efficient linear classifier suitable for high-dimensional sparse data.
- **Multilayer Perceptron (MLP)**: A simple feedforward neural network with hidden layers.

These models were trained on raw tabular data to establish baseline performance metrics.

B. Lightweight Deep Learning Models

To capitalize on the visual encoding, two pre-trained CNN architectures were employed using transfer learning:

- **EfficientNetB0**: Known for its compound scaling technique, EfficientNetB0 offers high performance with minimal computational cost. The top layer was removed, and a custom dense classifier was added to adapt it for binary classification.
- **InceptionV3**: A lightweight model that uses factorized convolutions and aggressive dimensionality reduction. It was also fine-tuned with a new classification head.

Both models were initialized with ImageNet weights and fine-tuned on the newly generated image dataset using transfer learning principles. Data augmentation techniques such as random rotation, zooming, and horizontal flipping were applied during training to improve generalization.

4. Results and Analysis

The experimental phase of this research is aimed at validating the effectiveness of the proposed framework — the integration of text-to-image conversion with lightweight deep learning models for intrusion detection. The experiments were conducted in a controlled environment to assess classification performance, computational efficiency, and robustness. This section presents detailed findings from model training, performance evaluation, and comparative analysis across traditional ML and modern DL architectures.

4.1 Training and Configuration

After converting the CAN data into image format, the dataset was split into 80% for training and 20% for testing. Both **EfficientNetB0** and **InceptionV3** were initialized with pre-trained ImageNet weights, and their top layers were replaced with a global average pooling layer, a dropout layer (rate = 0.4), and a final dense layer with a sigmoid activation function for binary classification.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The models were trained using the **Adam optimizer** with a learning rate of 0.0001. A batch size of 32 and up to 50 epochs were selected. Early stopping was implemented based on validation loss with a patience of 5 epochs to avoid overfitting. **Binary cross-entropy** was used as the loss function.

4.2 Comparative Performance with Machine Learning Models

Table 1 presents a comparative summary of the performance of five different models applied to an image-transformed intrusion detection dataset. Among the traditional machine learning models, Logistic Regression and SGD performed modestly with accuracy values of 87.3% and 85.6%, respectively. The Multilayer Perceptron (MLP) outperformed the other ML models, reaching 90.4% accuracy and 89.7% F1 score, highlighting the effectiveness of neural networks even in their shallow forms. However, the lightweight deep learning models, EfficientNetB0 and InceptionV3, exhibited significantly higher performance. EfficientNetB0 achieved the highest accuracy of 96.8% and an F1 score of 96.1%, while InceptionV3 followed closely with 95.2% and 94.5%, respectively. These results clearly demonstrate the superiority of deep learning techniques, particularly when paired with innovative data representation methods such as text-to-image conversion. The high F1 scores indicate the models' robust performance across both positive and negative classes, crucial for minimizing false alarms in IDS applications.

Table 1: Accuracy and F1 Score comparison of traditional machine learning models and deep learning models

Model	Accuracy (%)	F1 Score (%)
Logistic Regression	87.3	86.5
Stochastic Gradient Descent (SGD)	85.6	84.8
Multilayer Perceptron (MLP)	90.4	89.7
EfficientNetB0	**96.8**	**96.1**
InceptionV3	95.2	94.5

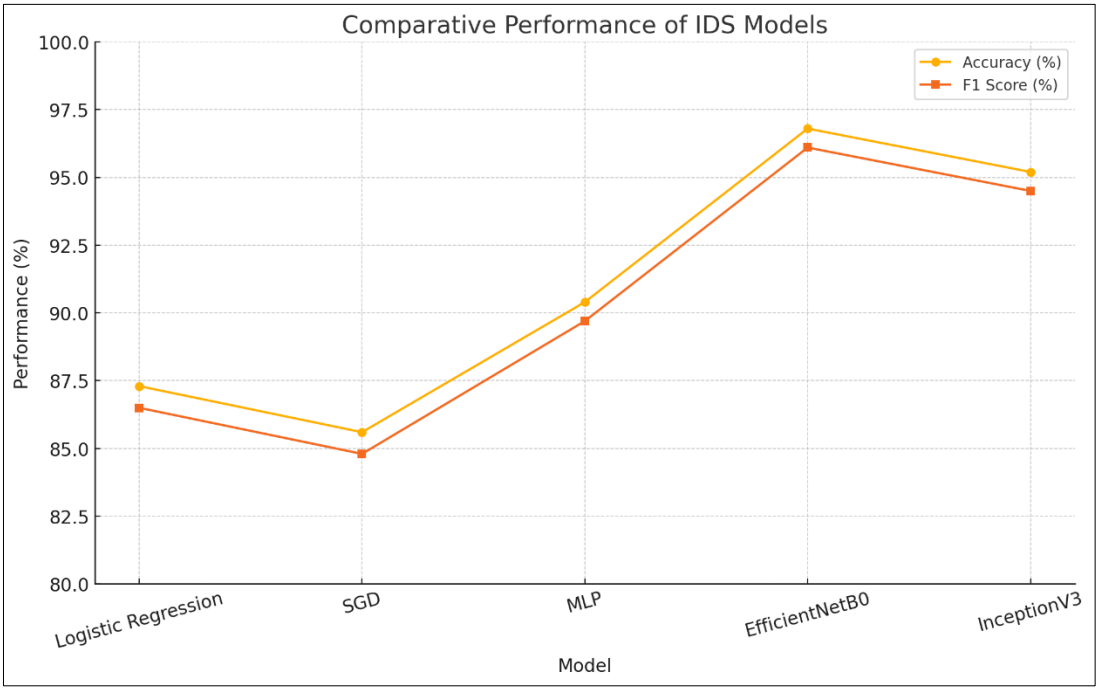

Figure 3: Comparative analysis of classification performance (Accuracy and F1 Score) of traditional machine learning models and deep learning models.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Figure 3. illustrate a performance comparison among five classification models applied to an intrusion detection system (IDS). Traditional machine learning models—Logistic Regression, Stochastic Gradient Descent (SGD), and Multilayer Perceptron (MLP)—demonstrate moderate accuracy and F1 scores, with MLP achieving the best performance among them (90.4% accuracy and 89.7% F1). In contrast, lightweight deep learning models significantly outperform traditional methods. EfficientNetB0 achieves the highest accuracy (96.8%) and F1 score (96.1%), followed closely by InceptionV3 with 95.2% accuracy and 94.5% F1. This substantial performance gain validates the effectiveness of the proposed text-to-image conversion and the use of transfer learning with efficient CNN architectures. The results confirm that deep models not only improve detection accuracy but also offer better generalization in identifying cyber threats. These findings underscore the viability of using lightweight DL models for real-time, resource-constrained IDS applications, particularly in automotive systems.

4.3 Computational Efficiency

In addition to classification performance, the runtime efficiency of the models was also evaluated. EfficientNetB0 required fewer parameters (~5.3M) compared to traditional CNNs like ResNet50 (~23M), and inference was completed in less than 50 ms per sample, making it viable for deployment in embedded systems.

4.4 Analysis

The experimental results demonstrate that converting tabular IDS data into image format enhances the ability of CNNs to learn complex attack patterns. The lightweight models not only maintain high accuracy but also ensure resource-efficient operation. The application of **SMOTE** during preprocessing contributed to balanced learning and reduced bias toward the majority class. The approach is especially suitable for domains like **automotive security**, where real-time response and limited computational resources are key constraints.

5. Applications

1. **Automotive Cybersecurity Systems**
   The proposed framework can be integrated into in-vehicle ECUs to detect malicious CAN messages in real time, protecting autonomous and connected vehicles from spoofing, DoS, and fuzzy attacks.
2. **Internet of Things (IoT) Security**
   Given its lightweight nature, the model is ideal for deployment in IoT devices where memory and computational capacity are limited. It can monitor device traffic and detect anomalies efficiently.
3. **Edge Computing-Based Intrusion Detection**
   The low-latency inference and reduced model size make this framework suitable for edge nodes in distributed networks, enabling decentralized intrusion detection without the need for cloud-based computation.
4. **Smart City Infrastructure**
   The approach can be used to secure communication between interconnected components in smart city networks, including traffic signals, surveillance systems, and public transportation units.
5. **Industrial Control Systems (ICS)**
   Industrial environments using networked control systems can benefit from the framework's ability to detect anomalies in sensor and actuator communications in real time.
6. **Healthcare IoMT Security**
   In Internet of Medical Things (IoMT) environments, the model can be used to monitor communication protocols between medical devices to detect unauthorized access or data tampering.
7. **Smart Grid and Energy Systems**
   The framework can be deployed in smart meters or substations to detect malicious control signals or unauthorized access attempts in critical infrastructure.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

6. Conclusion

This research work introduces a novel and efficient approach to intrusion detection by combining text-to-image conversion with lightweight deep learning architectures. The proposed framework addresses key challenges in modern IDS design, particularly in domains like automotive systems, where computational resources are limited and real-time performance is essential. By transforming structured CAN data into RGB image representations, we enable the use of powerful vision-based CNN models to extract rich spatial and contextual features from sequential message patterns. Among the models evaluated, EfficientNetB0 achieved the highest performance with 96.8% accuracy and 96.1% F1 score, while InceptionV3 also demonstrated strong results. These outcomes clearly surpass those of traditional machine learning models such as Logistic Regression, SGD, and MLP. Additionally, the application of SMOTE proved effective in mitigating class imbalance, further enhancing detection capability. Overall, the framework demonstrates that integrating visual data representation with lightweight transfer learning models is a promising direction for scalable, high-performance, and real-time IDS applications in embedded and automotive environments.

References

[1] P. Barnard, N. Marchetti, and L. A. DaSilva, "Robust network intrusion detection through explainable artificial intelligence (XAI)," IEEE Network Letters, vol. 4, pp. 167–171, 2022.

[2] S. Hariharan, R. R. Rejimol Robinson, R. R. Prasad, C. Thomas, and N. Balakrishnan, "XAI for intrusion detection system: Comparing explanations based on global and local scope," Journal of Computer Virology and Hacking Techniques, vol. 19, pp. 217–239, 2022.

[3] O. Arreche, T. R. Guntur, J. W. Roberts, and M. Abdallah, "E-XAI: Evaluating black-box explainable AI frameworks for network intrusion detection," IEEE Access, vol. 12, pp. 23954–23988, 2024.

[4] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," Journal of Sensor and Actuator Networks, vol. 12, p. 29, 2023.

[5] A. Awajan, "A novel deep learning-based intrusion detection system for IoT networks," Computers, vol. 12, p. 34, 2023.

[6] K. Roshan and A. Zafar, "Ensemble adaptive online machine learning in data stream: A case study in cyber intrusion detection system," International Journal of Information Technology, vol. 16, pp. 5099–5112, 2024.

[7] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection IDS for detecting DoS attacks in IoT networks based on machine learning algorithms," Sensors, vol. 24, p. 713, 2024.

[8] M. F. Saiyed and I. Al-Anbagi, "A genetic algorithm- and t-test-based system for DDoS attack detection in IoT networks," IEEE Access, vol. 12, pp. 25623–25641, 2024.

[9] A. K. Mishra, S. Paliwal, and G. Srivastava, "Anomaly detection using deep convolutional generative adversarial networks in the Internet of Things," ISA Transactions, vol. 145, pp. 493–504, 2023.

[10] S. Yadav, H. Hashmi, D. Vekariya, Z. A. Khan, and J. V. Fidelis, "Mitigation of attacks via improved network security in IoT network environment using RNN," Measurement: Sensors, vol. 32, p. 101046, 2024.

[11] M. Balega, W. Farag, X.-W. Wu, S. Ezekiel, and Z. Good, "Enhancing IoT security: Optimizing anomaly detection through machine learning," Electronics, vol. 13, p. 2148, 2024.

[12] A. Javed, A. Ehtsham, M. Jawad, M. N. Awais, A.-H. Qureshi, and H. Larijani, "Implementation of lightweight machine learning-based intrusion detection system on IoT devices of smart homes," Future Internet, vol. 16, p. 200, 2024.

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

[13] S. Yaras and M. Dener, "IoT-based intrusion detection system using new hybrid deep learning algorithm," Electronics, vol. 13, p. 1053, 2024.

[14] J. Li, M. S. Othman, H. Chen, and L. M. Yusuf, "Optimizing IoT intrusion detection system: Feature selection versus feature extraction in machine learning," Journal of Big Data, vol. 11, p. 36, 2024.

[15] D. Krishnan and P. Shrinath, "Robust botnet detection approach for known and unknown attacks in IoT networks using stacked multi-classifier and adaptive thresholding," Arabian Journal for Science and Engineering, vol. 49, pp. 12561–12577, 2024.

[16] J. B. Awotunde, S. O. Folorunso, A. L. Imoize, J. O. Odunuga, C.-C. Lee, C.-T. Li, and D.-T. Do, "An ensemble tree-based model for intrusion detection in industrial internet of things networks," Applied Sciences, vol. 13, p. 2479, 2023.

[17] Y. Alotaibi and M. Ilyas, "Ensemble-learning framework for intrusion detection to enhance internet of things' devices security," Sensors, vol. 23, p. 5568, 2023.

[18] O. Arreche, T. Guntur, and M. Abdallah, "XAI-IDS: Toward proposing an explainable artificial intelligence framework for enhancing network intrusion detection systems," Applied Sciences, vol. 14, p. 4170, 2024.

[19] Q. Yuan and N. Xiao, "Scaling-based weight normalization for deep neural networks," IEEE Access, vol. 7, pp. 7286–7295, 2019.

[20] J. Sun, X. Cao, H. Liang, W. Huang, Z. Chen, and Z. Li, "New interpretations of normalization methods in deep learning," in Proc. AAAI Conf. Artif. Intell., Vancouver, Canada, Feb. 2020, vol. 34, pp. 5875–5882.

[21] R. Guedrez, O. Dugeon, S. Lahoud, and G. Texier, "Label encoding algorithm for MPLS segment routing," in Proc. 2016 IEEE 15th Int. Symp. Network Comput. Appl. (NCA), Cambridge, MA, USA, Oct.–Nov. 2016, pp. 113–117.

[22] S. Ö. Arik and T. Pfister, "Tabnet: Attentive interpretable tabular learning," in Proc. AAAI Conf. Artif. Intell., Vancouver, Canada, Feb. 2021, vol. 35, pp. 6679–6687.