

Stacked Ensemble Deep Learning for Robust Intrusion Detection in IoT Networks

Marwa Amara^{1,2} ^a, Nadia Smairi² and Mohamed Jaballah²

¹*Department of Computer Sciences, Faculty of Sciences, Northern Border University, Arar, Saudi Arabia*

²*LARIA UR22ES01, ENSI, Manouba University, Tunisia*

Keywords: Stacked Ensemble Model, Class Imbalance, CICIDS2017 Dataset, Cyber Threat Detection.

Abstract: Intrusion Detection Systems (IDS) are critical for addressing the growing complexity of cyber threats in the Internet of Things (IoT) domain. This paper introduces a novel stacked ensemble approach combining Convolutional Neural Networks (CNN), Temporal Convolutional Networks (TCN), and Long Short-Term Memory (LSTM) models through a logistic regression meta-model. The proposed approach leverages the distinct strengths of each classifier; sequential pattern recognition by LSTMs, temporal dependency modeling by TCNs, and spatial feature extraction by CNNs to create a robust and reliable detection framework. To address the class imbalance problem, we applied various balancing techniques, including Oversampling, Undersampling, and a hybrid Meet-in-the-Middle method. The effectiveness of the approach is demonstrated on the CICIDS2017 dataset, achieving an accuracy of 99.99% and an F1-score of 100% with Oversampling, and 99.93% accuracy with the Meet-in-the-Middle technique.

1 INTRODUCTION

In the rapidly evolving domain of cybersecurity, IDS play a pivotal role in safeguarding networks against unauthorized access and increasingly sophisticated cyber threats. Traditional IDS approaches often struggle to adapt to the dynamic and evolving nature of modern cyber attacks, resulting in reduced effectiveness in real-world scenarios. To address these challenges, we introduce a novel ensemble learning-based approach that combines the strengths of multiple deep classifiers. Ensemble learning, a technique that integrates multiple learning algorithms, has proven to be transformative in the field of machine learning (Mohammed and Kora, 2023). By leveraging the diversity of multiple models, ensemble methods achieve superior prediction accuracy, particularly for complex tasks like intrusion detection. The aggregation of decision-making processes from various classifiers enables ensemble models to overcome the limitations of individual estimators and deliver robust and reliable predictions (Mohammed and Kora, 2023).

In this paper, we propose a Stacked Ensemble Deep Learning Approach, which integrates three powerful deep learning models: CNN, TCN, and LSTM. Each base classifier captures distinct aspects of the network traffic data—spatial patterns, temporal dependencies, and sequential behaviors, respectively.


These individual predictions are then combined in a stacked architecture. The logistic regression meta-model is trained on the meta-features generated by the base models, combining their predictions to optimize the final classification performance.

To address the prevalent issue of class imbalance in intrusion detection datasets, we evaluate three balancing techniques; Oversampling, Undersampling, and Meet-in-the-Middle approach. This comprehensive strategy ensures that the model maintains high generalization performance while reducing the risks of bias introduced by imbalanced data. The effectiveness of our proposed model is evaluated using well-established metrics, including accuracy, precision, recall, and F1-score.

The remainder of this paper is structured as follows: Section 2 offers a thorough examination of existing research in the field of IDS. In Section 2.1, we delve into our proposed ensemble model. The evaluation of our model's performance, is presented in Section 3. Finally, Section 4 summarizes our findings .

2 RELATED WORKS

This section explores the utilization of Deep learning (DL) in intrusion detection, highlighting its pivotal role in revolutionizing IDS. DL has demonstrated remarkable potential in enhancing the accuracy of

^a  <https://orcid.org/0000-0002-4521-0867>

IDS, providing advanced mechanisms to safeguard networks against evolving cyber threats.

Recent studies have proposed innovative approaches to leverage DL for intrusion detection. For instance, (Vijayanand et al., 2019) introduced an innovative attack detection system that leverages DL algorithms to scrutinize smart meter communications. This system employs a hierarchical arrangement of multi-layer DL algorithms, enhancing its ability to accurately pinpoint cyber-attacks. Similarly, (Lee and Hong, 2020) developed a DL-based algorithm targeting Dynamic Link Library (DLL) injection attacks in SCADA systems, utilizing Windows API functions to detect and mitigate such threats. In addition, (Li and Hedman, 2019) proposed monitoring techniques for detecting irregularities in branch flows and load deviations, addressing false data injection (FDI) attacks through a two-pronged detection method. Focusing on SCADA security, (Aldossary et al., 2021) employed Bidirectional Long Short-Term Memory (Bi-LSTM) to effectively detect denial-of-service (DoS) attacks. Expanding on DL applications, (Agarwal et al., 2021) combined deep neural networks (DNNs) with a feature selection-whale optimization algorithm, achieving high accuracy in DDoS detection. Exploring various algorithms for cybersecurity identification, (Ahakonye et al., 2021) found that decision tree and K-nearest neighbor algorithms (KNN) yielded satisfactory results in cybersecurity identification. Advancing the field further, (Farrukh et al., 2021) proposed a two-tier hierarchical machine learning model. This model demonstrated a remarkable 95.44% accuracy in detecting cyber-attacks. It operates by first distinguishing between normal and cyberattack modes in its initial layer, thereby streamlining the detection process. For Software Defined Networking, (Fouladi et al., 2022) offered a DDoS attack detection and countermeasure technique using discrete wavelet transform (DWT) and an auto-encoder neural network. In pursuit of optimal feature selection for IDS, (Fatani et al., 2021) employed a swarm intelligence technique alongside an Aquila optimizer model, yielding reasonable results with a CNN classifier integrated with a particle swarm optimization model (PSO). In a notable contribution to Smart Grid security, (Diaba and Elmusrati, 2023), developed a hybrid DL algorithm to enhance the security of the Smart Grid against Distributed DoS attacks. This algorithm integrates the strengths of CNNs and Gated Recurrent Unit models. Simulation tests using a cybersecurity dataset from the Canadian Institute of Cybersecurity showed that this novel algorithm surpasses existing IDS, achieving an impressive overall accuracy rate of 99.7%.

Reflecting on the diverse approaches in cybersecurity, various researchers have proposed DL models for intrusion detection, each with distinct findings and limitations. (Alzughabi and El Khediri, 2023) developed a DNN using Backpropagation, trained on the CSE-CICIDS2018 dataset, and achieved 98.41% accuracy in multiclass classification. However, the model's validation was limited to a single dataset, raising questions about its broader applicability. Additionally, the study did not address training and validation times, which are crucial for further research.

Similarly, (Thakkar and Lohiya, 2023) also proposed a Deep neural network (DNN), training it on NSL-KDD, UNSWNB-15, and CIC-IDS-2017 datasets. The model achieved accuracies of 99.84%, 89.03%, and 99.80%, respectively. Despite its high detection rate, the model's training time was lengthy, and validation time was not reported.

Addressing the need for more current and comprehensive dataset validation, (Sharma et al., 2023) presented a DNN trained on the NSL-KDD dataset, attaining a 99.3% accuracy rate. However, the model lacked validation with newer and larger datasets, and the study did not provide information on training and validation durations.

Innovating in model optimization, (El-Ghamry et al., 2023) introduced an optimized CNN model, VGG16-PSO, for intrusion detection, trained and validated using the NSL-KDD dataset. While the model showed excellent performance, it was evaluated using a dataset over two decades old, and the study did not disclose the time consumed for training and validation.

(Wu and Chen, 2023) proposed a simple DNN that achieved a 97% accuracy rate. The validation of this model was restricted to the CSE-CICIDS2018 dataset, and the study omitted details on training and inference times.

Likewise, (Hnamte et al., 2023) proposed an LSTM-AE model, trained and validated using CICIDS2017 and CSE-CICIDS2018, achieving 99.99% and 99.10% accuracy, respectively. The training time for the model was lengthy and required high-end computing for larger datasets. Continuing the trend of model innovation, (Chanu et al., 2023) developed an MLP-GA model that achieved a 98.9% detection accuracy rate. However, the model's validation was limited to the CICIDS2017 dataset, and its accuracy decreased when validated with newer, larger datasets. In contrast, (Hnamte and Hussain, 2023a), a DC-NNBiLSTM model was proposed and trained on CICIDS2018 and EDGEIIoT 2 datasets, achieving 100% and 99.64% accuracy, respectively. The model was also compared with other models in terms of ac-

curacy, loss rate, training time, and inference time, both on CPU and GPU. Despite its high accuracy, the model was complex and had a lengthy training duration.

In a significant breakthrough, (Hnamte and Husain, 2023b). developed an intrusion detection framework leveraging deep CNNs. Trained on extensive datasets, the DCNN model achieves detection accuracy levels between 99.79% and 100%. Its effectiveness is validated using four distinct IDS datasets, including ISCX-IDS 2012 and CICIDS2018.

Similarly, (Patthi et al., 2024) introduced a two-layer classification model combining KNN and SVMs. The first layer categorizes data into Normal, Major, and Minor Attack groups, while the second layer further classifies Major and Minor Attacks. Tested on the NSL-KDD dataset, the model notably excels in detecting Minor Attacks.

Addressing IoT networks' vulnerability, (Latif et al., 2024) proposed a DL model for intrusion detection, tested on NSL-KDD and UNSW-NB 15 datasets, demonstrating superior accuracy. This study incorporated explainable AI techniques like LIME and SHAP for model interpretability.

In the context of the Smart Healthcare System and IoMT, (Alzubi et al., 2024) introduced a novel IDS solution employing a DL framework that combines CNN and LSTM, tested on the CSE-CIC-IDS 2018 dataset, and demonstrated superior accuracy compared to existing methods.

While these works highlight the transformative potential of DL in IDS, several critical gaps persist. First, many studies focus on individual DL architectures, limiting their ability to fully capture the diverse patterns in network traffic, such as spatial, temporal, and sequential dependencies. This lack of synergy between different DL architectures often results in suboptimal performance, particularly for complex attack scenarios. Second, much of the existing research overlooks the challenge of unbalanced datasets, which are common in intrusion detection scenarios. This neglect raises concerns about model robustness and the ability to generalize effectively to real-world data distributions.

Our proposed stacked ensemble approach directly addresses these challenges by integrating three models into a unified framework. Our method provides a holistic analysis of network traffic, significantly enhancing detection accuracy. Moreover, the inclusion of balancing techniques, such as Oversampling, Undersampling, and the Meet-in-the-Middle method, further strengthens the model's ability to handle imbalanced data, a common challenge in IDS.

2.1 Proposed Approach

In addressing the complexities of IoT intrusion detection, our approach utilizes a stacked ensemble model to integrate multiple DL models, each designed to capture unique patterns within network traffic data. By combining the spatial feature recognition capabilities of a CNN, TCN, and the sequential pattern analysis of LSTM, our method ensures a comprehensive understanding of both benign and malicious traffic. This ensemble approach, visualized in Figure 1, allows each base model to contribute distinct insights, which are then optimized through a meta-model for enhanced accuracy.

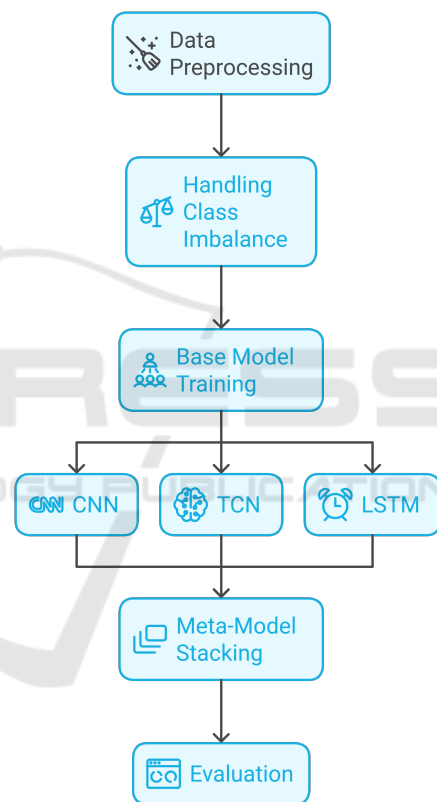


Figure 1: Stacked Ensemble Model Architecture for IoT Intrusion Detection.

Such a layered strategy enables the system to adapt to diverse IoT traffic behaviors, resulting in more reliable and balanced classification. The algorithm 1 outlines the steps of our stacked ensemble approach for IoT intrusion detection.

This algorithm is followed by a detailed breakdown of each component, highlighting the importance of base models, the construction of the meta-feature matrix, and the role of the meta-model in refining classification accuracy.

Data: Balanced IoT dataset \mathbf{D} after preprocessing

Result: Final classification \hat{y} of traffic as benign or malicious

Step 1: Train Base Models
for each base model
 $M_i \in \{CNN, TCN, LSTM\}$ **do**
 Train M_i on \mathbf{D}_{train} ;
 Obtain predictions \hat{y}_{M_i} for each sample in \mathbf{D}_{train} ;
end

Step 2: Construct Meta-Feature Matrix
 Combine $\hat{y}_{CNN}, \hat{y}_{TCN}, \hat{y}_{LSTM}$ into meta-feature matrix \mathbf{F} ;

Step 3: Train Meta-Model
 Train logistic regression (LR) on \mathbf{F} to learn optimal weights for $\{\hat{y}_{M_i}\}$;

Step 4: Evaluate Stacked Model
for each sample x_j in \mathbf{D}_{test} do
 Obtain final classification $\hat{y}_j = LR(\mathbf{F}_j)$;
 Calculate evaluation metrics: Accuracy, Precision, Recall, F1-Score;
end

Output: Final classifications $\{\hat{y}_j\}$ for all samples in \mathbf{D}_{test} ;

Algorithm 1: Stacked Ensemble Model for IoT Intrusion Detection.

2.1.1 Data Preprocessing

In IoT-based intrusion detection, preparing the data is essential for reliable performance of machine learning classifiers. Raw network traffic data often includes inconsistencies such as missing values, infinities, duplicates, and features that provide no useful information. These issues can interfere with a model's ability to correctly identify attacks, so an effective preprocessing process is critical to create streamlined dataset. The figure 2 summarizes the cleaning steps in the pre-processing phase, which ultimately improves model performance and robustness in distinguishing between benign and malicious IoT traffic.

The preprocessing procedure begins by standardizing column names by stripping extra spaces for consistency. Negative values are replaced with zero to maintain logical bounds. Duplicate rows are removed to ensure the dataset is free from repetitive information. Columns with zero variance(those containing the same value for every record) are also eliminated, as they add no value to the learning process and can unnecessarily increase computational overhead. Infinite values, which can disrupt calculations, are replaced with NaNs, and rows containing NaNs are removed to ensure a complete dataset. Finally, identi-

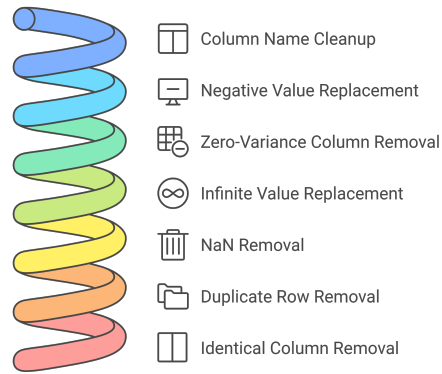


Figure 2: Data Preprocessing for Attack Detection.

cal columns are eliminated to streamline the data and improve efficiency. The result of this preprocessing phase is a simplified and consistent dataset, prepared for feature selection and classifier training. This careful preparation helps improve the model's ability to detect intrusions accurately by allowing it to focus on meaningful patterns in the data.

2.2 Data Imbalance Handling

In IoT intrusion detection, class imbalance is a prevalent issue, with benign traffic often significantly outnumbering malicious samples. To handle this challenge, we tested multiple resampling techniques, including the oversampling, undersampling, and meet-in-the-middle approach. Each technique provides a unique way to balance the classes (Islam and Mustafa, 2023), and we evaluated each method to identify the most effective approach for our dataset. To ensure the integrity of the evaluation, the dataset was split into 80% training data and 20% test data, with all resampling techniques applied exclusively to the training data to prevent data leakage into the test set. Oversampling duplicates instances from the minority class (malicious traffic) until its size matches that of the majority class (benign traffic), resulting in equal representation of both classes in the training data. This method can be represented mathematically as:

$$N'_{\text{minority}} = N_{\text{majority}} \quad (1)$$

where N'_{minority} is the new size of the minority class after oversampling, and N_{majority} is the size of the majority class. Undersampling, in contrast, reduces the size of the majority class by randomly selecting a subset of instances, equalizing it with the minority class. This technique is represented as:

$$N'_{\text{majority}} = N_{\text{minority}} \quad (2)$$

where N'_{majority} is the new size of the majority class, which helps prevent the model from favoring the ma-

jority class, though it results in a smaller, balanced dataset.

Finally, we implemented a custom approach called meet-in-the-middle, which balances the classes by finding a midpoint between the sizes of the majority and minority classes. This method involves under-sampling the majority class to the midpoint size and oversampling the minority class to match this size, avoiding excessive duplication or data loss. The midpoint M is calculated as:

$$M = \frac{N_{\text{majority}} + N_{\text{minority}}}{2} \quad (3)$$

where M is the target class size after resampling, and N_{majority} and N_{minority} represent the original sizes of the majority and minority classes, respectively.

Each resampling technique was evaluated based on key metrics, including accuracy, precision, recall, and F1-score. By comparing these metrics, we identified the most effective technique, enhancing the model's ability to distinguish effectively between benign and malicious traffic.

2.3 Base Models and Stacking Ensemble Approach

Our methodology leverages a stacked ensemble approach using three DL base models; CNN, TCN, and LSTM, to capture diverse aspects of IoT data patterns. Each model is trained on resampled datasets, enabling the ensemble to harness unique feature representations for improved performance in detecting network anomalies.

The CNN model extracts local feature patterns from the data, detecting specific types of network traffic anomalies. Mathematically, the convolutional operation in a CNN is given by:

$$h_{ij} = f \left(\sum_{m=1}^M w_m x_{i+m-1,j} + b \right) \quad (4)$$

where h_{ij} represents the output feature map, w_m is the convolutional kernel, $x_{i+m-1,j}$ represents the input data, and b is the bias term. The CNN's hierarchical spatial properties allow it to identify patterns in high-dimensional network traffic data effectively.

The TCN model, which incorporates dilated convolutions, captures long-range dependencies in sequential IoT data. This allows the TCN to recognize temporal patterns across extended periods, which is valuable for network traffic analysis. The dilated convolution in a TCN is mathematically expressed as:

$$y(t) = \sum_{k=0}^{K-1} w_k x(t - d \cdot k) \quad (5)$$

where $y(t)$ is the output at time t , w_k are the filter weights, $x(t - d \cdot k)$ is the input at the dilated time step, and d is the dilation factor. By adjusting d , the TCN can capture dependencies across various time spans.

The LSTM model, known for its memory cell and gating mechanisms, captures sequential dependencies in the network traffic, effectively recognizing temporal patterns present in IoT traffic. The LSTM cell updates are formulated as:

$$c_t = f_t \odot c_{t-1} + i_t \odot \tilde{c}_t \quad (6)$$

where c_t is the cell state at time t , f_t , i_t , and \tilde{c}_t are the forget, input, and candidate cell states, respectively, and \odot denotes element-wise multiplication. This update mechanism allows the LSTM to retain information over long sequences, making it effective for sequential data like network traffic.

Each of these base models is trained independently on resampled versions of the dataset. Their outputs, representing predictions for each input instance, form a matrix of meta-features, $\mathbf{F} \in \mathbb{R}^{n \times m}$, where n is the number of samples and m is the number of base models. Let $f_i(X)$ denote the prediction from the i -th base model for input X , then:

$$\mathbf{F} = \begin{bmatrix} f_1(X_1) & f_2(X_1) & \dots & f_m(X_1) \\ f_1(X_2) & f_2(X_2) & \dots & f_m(X_2) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(X_n) & f_2(X_n) & \dots & f_m(X_n) \end{bmatrix} \quad (7)$$

The meta-feature matrix \mathbf{F} is then used to train a Logistic Regression model, $g(\mathbf{F})$, which serves as the meta-model. The logistic regression learns a weighted combination of the base models' predictions to yield a final classification decision. Mathematically, the meta-model's prediction \hat{y} is:

$$\hat{y} = g(\mathbf{F}) = \sigma \left(\sum_{j=1}^m \alpha_j f_j(X) + \beta \right) \quad (8)$$

where σ is the logistic sigmoid function, α_j are the learned weights for each base model's predictions, and β is the bias term.

By combining predictions from each base model, the meta-model leverages their complementary strengths, resulting in improved overall performance. This stacked ensemble approach enhances classification robustness, as each model contributes unique insights into the data. The CNN captures local spatial patterns, the TCN detects long-term dependencies, and the LSTM captures sequential patterns. The meta-model effectively integrates these diverse representations, leading to more accurate and reliable intrusion detection.

3 EXPERIMENTAL RESULTS

In this section, we evaluate the performance of the proposed stacked ensemble model across different class balancing techniques: Oversampling, Undersampling, and Meet-in-the-Middle.

3.1 Dataset Description

The CICIDS2017 dataset (Sharafaldin et al., 2018), a benchmark for intrusion detection, was used for our experiments. The dataset includes network traffic labeled as normal or one of several types of attacks. For binary classification (Figure 3), all attack types were grouped under a single 'anomaly' label, while normal traffic was labeled 'benign'.

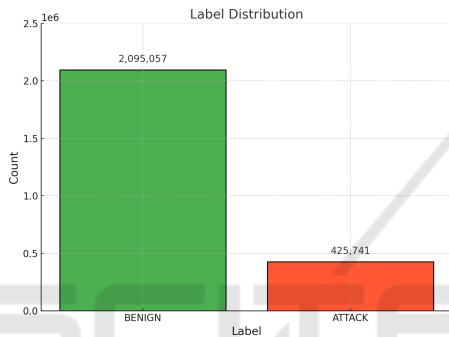


Figure 3: Class Distribution of the CICIDS2017 Dataset .

This study focuses on traffic patterns and anomalies observed on Friday, a subset of the dataset that captures both routine network behavior and complex intrusion scenarios. Preprocessing steps, including handling missing values, feature scaling, and dataset balancing, were applied to prepare the data for robust training and evaluation.

3.2 Stacked Model Performance

The stacked ensemble model, combining CNN, TCN, and LSTM predictions through a logistic regression meta-model, significantly improves classification performance. By leveraging the strengths of each base model; spatial features from CNN, temporal dependencies from TCN, and sequential patterns from LSTM, the stacked model achieves near-perfect classification metrics. Across all balancing techniques, the stacked model demonstrates strong performance, with accuracy exceeding 99.9% and minimal misclassifications, as shown in Figure 4. These results confirm the effectiveness of the stacked ensemble approach, particularly in maintaining high precision and recall even under challenging conditions such as imbalanced data. To further evaluate the balancing

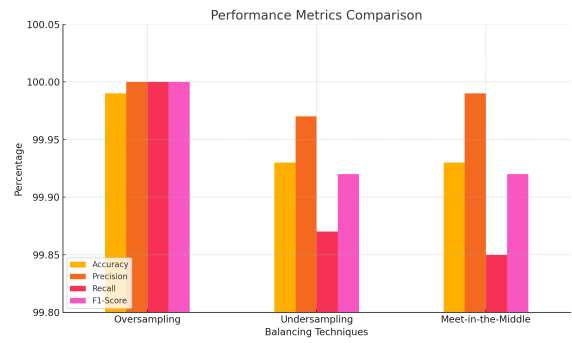


Figure 4: Performance Metrics Comparison Across Balancing Techniques.

techniques, we analyze the confusion matrices, ROC curves, and precision-recall metrics for each method.

Table 1 presents the True Positive Rate (TPR), False Positive Rate (FPR), and key confusion matrix values for each balancing technique. While Oversampling achieves perfect classification (TPR = 100%, FPR = 0%), the Meet-in-the-Middle approach provides a highly balanced performance with the lowest FPR of 0.004%, demonstrating its robustness in handling class imbalance.

Table 1: Confusion Matrix Metrics for Balancing Techniques.

Technique	TP	FP	TN	FN	TPR (%)	FPR (%)
Oversampling	18201	0	24555	0	100.00	0.00
Undersampling	18177	5	24550	24	99.87	0.02
Meet-in-the-Middle	18174	1	24554	27	99.85	0.004

The ROC curves in Figure 5 compare the performance of the stacked model across the three balancing techniques.

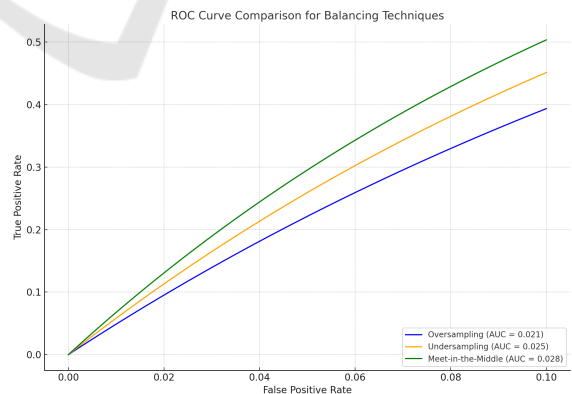


Figure 5: ROC Curves Comparing Balancing Techniques.

The ROC curves in Figure 5 illustrate the performance of the stacked model across the three balancing techniques. The **Area Under the Curve (AUC)** quantifies the overall performance of a model by summarizing the trade-off between TPR (sensitivity) and

FPR across all thresholds. Mathematically, it is computed as:

$$AUC = \int_0^1 TPR(t), d(FPR(t)) \quad (9)$$

AUC values range from 0 to 1, with higher AUCs indicating better model performance in distinguishing between classes. Among the evaluated techniques, the Meet-in-the-Middle approach achieves the highest AUC of 0.028, demonstrating the best trade-off between TPR and FPR and highlighting its robustness in handling class imbalance under realistic conditions. While Oversampling (AUC = 0.021) and Undersampling (AUC = 0.025) also perform well, the marginal advantage of the Meet-in-the-Middle method underscores its effectiveness in maintaining generalization and robust classification.

3.3 Performance Comparison and Discussion

As a final evaluation of the results presented, we compare our proposed approach with other similar methods in the literature.

Table 2: Comparison of Our Proposed Stacked Ensemble Model with Existing Methods in Literature.

Authors	Method	Ensemble	Accuracy (%)
(Kumar et al., 2021b)	DLTIF	No	99.9
(Latif et al., 2021)	DnRaNN	No	98.5
(Kumar et al., 2021a)	Stacking	Yes	96.3
(Khan et al., 2023)	Stacking	Yes	98.5
(Gad et al., 2022)	XGBoost	Yes	99.1
Proposed (Oversampling)	Stacked	Yes	99.99
Proposed (Undersampling)	Stacked	Yes	99.93
Proposed (Meet-in-the-Middle)	Stacked	Yes	99.93

Our proposed stacked ensemble model demonstrates superior performance compared to existing state of the art methods in IoT intrusion detection, as shown in Table 2. Traditional approaches, such as DLTIF and XGBoost, achieve notable accuracy levels (99.9% and 99.1%, respectively); however, they lack the synergistic benefits of ensemble techniques. By combining the strengths of CNN, TCN, and LSTM models, our proposed stacked approach effectively captures diverse network traffic patterns, resulting in improved detection accuracy. Specifically, our model achieves an accuracy of 99.99% with the Oversampling technique, outperforming all previously reported methods. Additionally, the Meet-in-the-Middle and Undersampling approaches demonstrate balanced accuracy levels of 99.93%, providing a robust trade-off that mitigates overfitting while maintaining reliable classification performance. These results underscore the effectiveness of leveraging en-

semble methods to address class imbalance and enhance overall intrusion detection accuracy.

4 CONCLUSION

In this paper, we proposed a stacked ensemble model for IoT intrusion detection, combining the strengths of CNN, TCN, and LSTM models through a logistic regression meta-model. The approach effectively addresses the challenges of imbalanced data and captures diverse data patterns. By employing different balancing techniques, such as Oversampling, Undersampling, and Meet-in-the-Middle, we demonstrated that the Meet-in-the-Middle approach provides the best balance between precision and recall. The robustness and efficiency of the stacked model validate its suitability for real-world IoT environments, where high precision and low false positive rates are critical.

While the proposed model excels in binary classification for a subset of the CICIDS2017 dataset, future work will extend the analysis to the entire dataset for a more comprehensive evaluation. Additionally, multiclass classification and advanced techniques like ablation studies and cross-dataset domain adaptation will be explored to validate and enhance the model's generalizability.

REFERENCES

- Agarwal, A., Khari, M., and Singh, R. (2021). Detection of ddos attack using deep learning model in cloud storage application. *Wireless Personal Communications*, pages 1–21.
- Ahakonye, L. A. C., Nwakanma, C. I., Lee, J.-M., and Kim, D.-S. (2021). Efficient classification of enciphered scada network traffic in smart factory using decision tree algorithm. *IEEE Access*, 9:154892–154901.
- Aldossary, L. A., Ali, M., and Alasaadi, A. (2021). Securing scada systems against cyber-attacks using artificial intelligence. In *2021 international conference on innovation and intelligence for informatics, computing, and technologies (3ICT)*, pages 739–745. IEEE.
- Alzubi, J. A., Alzubi, O. A., Qiqieh, I., and Singh, A. (2024). A blended deep learning intrusion detection framework for consumable edge-centric iomt industry. *IEEE Transactions on Consumer Electronics*.
- Alzughairi, S. and El Khediri, S. (2023). A cloud intrusion detection systems based on dnn using backpropagation and pso on the cse-cic-ids2018 dataset. *Applied Sciences*, 13(4):2276.
- Chanu, U. S., Singh, K. J., and Chanu, Y. J. (2023). A dynamic feature selection technique to detect ddos attack. *Journal of Information Security and Applications*, 74:103445.

- Diaba, S. Y. and Elmusrati, M. (2023). Proposed algorithm for smart grid ddos detection based on deep learning. *Neural Networks*, 159:175–184.
- El-Ghamry, A., Darwish, A., and Hassanien, A. E. (2023). An optimized cnn-based intrusion detection system for reducing risks in smart farming. *Internet of Things*, 22:100709.
- Farrukh, Y. A., Ahmad, Z., Khan, I., and Elavarasan, R. M. (2021). A sequential supervised machine learning approach for cyber attack detection in a smart grid system. In *2021 North American Power Symposium (NAPS)*, pages 1–6. IEEE.
- Fatani, A., Dahou, A., Al-Qaness, M. A., Lu, S., and Elaziz, M. A. (2021). Advanced feature extraction and selection approach using deep learning and aquila optimizer for iot intrusion detection system. *Sensors*, 22(1):140.
- Fouladi, R. F., Ermiş, O., and Anarim, E. (2022). A ddos attack detection and countermeasure scheme based on dwt and auto-encoder neural network for sdn. *Computer Networks*, 214:109140.
- Gad, A. R., Haggag, M., Nashat, A. A., and Barakat, T. M. (2022). A distributed intrusion detection system using machine learning for iot based on ton-iot dataset. *International Journal of Advanced Computer Science and Applications*, 13(6).
- Hnamte, V. and Hussain, J. (2023a). Dnnbilstm: An efficient hybrid deep learning-based intrusion detection system. *Telematics and Informatics Reports*, 10:100053.
- Hnamte, V. and Hussain, J. (2023b). Dependable intrusion detection system using deep convolutional neural network: A novel framework and performance evaluation approach. *Telematics and Informatics Reports*, 11:100077.
- Hnamte, V., Nhung-Nguyen, H., Hussain, J., and Hwa-Kim, Y. (2023). A novel two-stage deep learning model for network intrusion detection: Lstm-ae. *IEEE Access*.
- Islam, M. T. and Mustafa, H. A. (2023). Multi-layer hybrid (mlh) balancing technique: A combined approach to remove data imbalance. *Data & Knowledge Engineering*, 143:102105.
- Khan, F., Jan, M. A., Alturki, R., Alshehri, M. D., Shah, S. T., and ur Rehman, A. (2023). A secure ensemble learning-based fog-cloud approach for cyberattack detection in iomt. *IEEE Transactions on Industrial Informatics*, 19(10):10125–10132.
- Kumar, P., Gupta, G. P., and Tripathi, R. (2021a). An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks. *Computer Communications*, 166:110–124.
- Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., and Hassan, M. M. (2021b). Dltif: Deep learning-driven cyber threat intelligence modeling and identification framework in iot-enabled maritime transportation systems. *IEEE Transactions on Intelligent Transportation Systems*, 24(2):2472–2481.
- Latif, S., Boulila, W., Koubaa, A., Zou, Z., and Ahmad, J. (2024). Dtl-ids: An optimized intrusion detection framework using deep transfer learning and genetic algorithm. *Journal of Network and Computer Applications*, 221:103784.
- Latif, S., e Huma, Z., Jamal, S. S., Ahmed, F., Ahmad, J., Zahid, A., Dashtipour, K., Aftab, M. U., Ahmad, M., and Abbasi, Q. H. (2021). Intrusion detection framework for the internet of things using a dense random neural network. *IEEE Transactions on Industrial Informatics*, 18(9):6435–6444.
- Lee, J.-M. and Hong, S. (2020). Keeping host sanity for security of the scada systems. *IEEE Access*, 8:62954–62968.
- Li, X. and Hedman, K. W. (2019). Enhancing power system cyber-security with systematic two-stage detection strategy. *IEEE Transactions on Power Systems*, 35(2):1549–1561.
- Mohammed, A. and Kora, R. (2023). A comprehensive review on ensemble deep learning: Opportunities and challenges. *Journal of King Saud University-Computer and Information Sciences*.
- Patthi, S., Singh, S., et al. (2024). 2-layer classification model with correlated common feature selection for intrusion detection system in networks. *Multimedia Tools and Applications*, pages 1–26.
- Sharafaldin, I., Lashkari, A. H., Ghorbani, A. A., et al. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, 1:108–116.
- Sharma, B., Sharma, L., and Lal, C. (2023). Anomaly-based dnn model for intrusion detection in iot and model explanation: Explainable artificial intelligence. In *Proceedings of Second International Conference on Computational Electronics for Wireless Communications: ICCWC 2022*, pages 315–324. Springer.
- Thakkar, A. and Lohiya, R. (2023). Fusion of statistical importance for feature selection in deep neural network-based intrusion detection system. *Information Fusion*, 90:353–363.
- Vijayanand, R., Devaraj, D., and Kannapiran, B. (2019). A novel deep learning based intrusion detection system for smart meter communication network. In *2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, pages 1–3. IEEE.
- Wu, C.-s. and Chen, S. (2023). A heuristic intrusion detection approach using deep learning model. In *2023 International Conference on Information Networking (ICOIN)*, pages 438–442. IEEE.