Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Adaptive Hybrid Deep Learning Model for Real-Time Anomaly Detection in IoT Networks

Esraa Saleh Alomari[1,*], Selvakumar Manickam[2], Mohammed Anbar[1]

[1] Computer Department, College of Education for Pure Sciences, Wasit University, 52001 Al-Kut, Wasit, Iraq
[2] National Advanced IPv6 Centre (NAv6), Universiti Sains Malaysia, Gelugor 11800, Penang, Malaysia

ARTICLE INFO

Article history:
Received23 January 2025
Received in revised form 1 July 2025
Accepted 10 July 2025
Available online 20 July 2025

ABSTRACT

The exponential growth of the internet of things (IoT) networks has posed great challenges in maintaining security because of the diverse and dynamic nature of connected devices. These complex environments often defeat traditional anomaly detection methods. In this paper, we present an adaptive hybrid deep learning framework incorporating Variational Autoencoders (VAEs) and Deep Neural Networks (DNNs) enhanced by XGBoost for feature selection for real-time anomaly detection and classification in IoT networks. The VAE component efficiently reduces high dimensional input data into a lower-dimensional latent space that maintains essential network traffic features while managing information loss for storage optimization and improved accuracy in detecting anomalies. Afterward, XGBoost is utilized to choose top 10 significant features with respect to feature selection. The DNN portion uses these latent features to detect as well as classify anomalies; it is therefore trained on how to identify complex patterns within the selected latent features so as to effectively tell apart malicious activities from normal network behaviors. Test Accuracy of 92.8% was achieved by the proposed VAE-DNN model, which displays its efficiency in IoT real-time anomaly detection. Mode also helps improve model accuracy when coupled with XGBoost based feature selection techniques

Keywords:
IoT Networks; Anomaly detection; Deep learning; VAE; RNN

1. Introduction

The internet of things (iot) allows sensors and smart devices to exchange information autonomously, which demands near real-time data processing capabilities [1]. In this way, a new type of analytics might be needed that can run on the limited computing resources though. An effective method for doing this is identifying anomaly behaviors - sometimes called outliers or events – which highlight odd patterns or states within a given system [2]. They happen at different points including on iot network edges up to dcs where reliable detection is essential for cleaning and classification purposes of data. The extra importance of anomalous event detection lies in the fact that detection of rare anomalies in iot data can offer significant actionable insights in various domains such as

[*] *Corresponding author.*
E-mail address: ealomari@uowasit.edu.iq

https://doi.org/10.37934/ard.137.1.278289

healthcare, manufacturing, finance, traffic management, energy among others [3]. In betting and gaming industry, for example, anomaly detectors are applied to signal some aspects implying insider trading. Similarly, these algorithms monitor machinery looking for any irregularities thereby ensuring production safety in industrial settings. However, most of the present techniques of anomaly detection in iot environments require substantial human interaction and are often tuned to local solutions [4]. In simple terms, experts can recognize any data that is out of place. Creating automated systems for detecting anomalies in iot has several hurdles [5]. One of the main challenges is having precise definitions and categories for all forms of anomalous data, especially in situations where there is a dearth or lack of labeled training data. Besides, normal behavior changes with time; this includes patterns in electricity consumption due to shifts in household occupancy. In the iot, anomalies are defined as deviations from expected or normal behaviors of devices, systems, or network traffic. These deviations signal potential disruptions such as operational failures, security intrusions, or inefficiencies that could compromise the functionality and safety of iot environments. Anomalies can manifest in various forms: a point anomaly indicates a single data instance that is significantly different from the majority; a contextual anomaly, relevant to specific conditions, may not be anomalous under different circumstances; and collective anomalies, where a group of related data points diverges from expected patterns when evaluated together [1]. Detecting these anomalies accurately is crucial for maintaining the reliability and security of iot systems. The effectiveness of anomaly detection systems in the iot heavily depends on the quality of ground truth labels used for training and evaluating models. These labels, which distinguish between normal and anomalous behavior, must be accurate and comprehensive to train machine learning models effectively. Any inaccuracies in these labels can lead to models that either miss actual anomalies or flag normal behavior as anomalous, undermining system reliability. Moreover, labels must cover a diverse range of anomalies, including subtle and rare occurrences, to ensure the model's robustness and its ability to generalize across different scenarios. The process of label generation should also be dynamic, adapting to new patterns and evolving threats in iot contexts to remain relevant. Additionally, the data used for these labels should be devoid of biases that could skew model training, such as imbalanced distributions between normal and anomalous examples. Therefore, maintaining high standards in the accuracy, coverage, timeliness, and objectivity of ground truth labels is essential for developing effective anomaly detection capabilities in iot networks [4].

This paper presents an adaptive deep learning model that combines deep neural networks (dnns) with variational autoencoders (vaes), and further includes feature selection with xgboost, for anomaly detection and classification in real-time iot networks. In this proposed framework, the critical capability of vaes is to capture meaningful latent features from high dimensional iot data while dnns are effective in detecting attacks and classifying different types of cyber-attacks. The vae portion will encode the high dimensional input data into a lower-dimensional latent space thereby keeping only relevant characteristics but ensuring it maintains useful information as well. The objective behind reducing is to ensure storage requirements are met yet maintain recognition accuracy even though some original information may loss eventually.

The dnn component follows the processing of the already extracted latent features, which are further examined for the detection of anomalies and identification steps for the classification of malicious activities. The power of a dnn in learning complex patterns and relationships among features is of the essence in that, hitherto, it finally leads to the effective differentiation of normal and malicious network behaviors. Such an integrated vae-dnn model can allow the development of an effective, efficient, and lightweight intrusion detection system in the iot environment.

Contributions in this paper, the main contributions of the proposed work are as follows:
• presentation of a lightweight intrusion detection model for iot networks making proper use of the

deep vae model to perform both anomaly detection and feature reduction. This is in slight contrast to most other existing methods, which mostly rely on aes to perform just one of the purposes. Herein, as in our experimental setup, we perform intense evaluations on real data by using ddosdataset covering both normal and malicious network traffic. The performance of the classification is measured across five iot devices using metrics like accuracy, precision, recall, f1 score, and execution time. Lastly, the efficiency of the proposed ids system is compared with state-of-the-art methods to show its effectiveness in detecting anomalies and classifying them within an iot network.

1.1 Related Work

Svm was already demonstrated as efficient in data classification and anomaly detection, whereas its efficiency was not yet separately estimated [6, 7] with the use of dcnns and many other models of ml. These kinds of dynamism and diversity in iot applications and its environments more enhance the need to find appropriate anomaly detection models for iot. In this light, the necessity arises to validate ml-based anomaly detection models across multiple datasets originating out of different environments. To validate the model, three most recent, up-to-date state-of-the-art datasets have been used: iot-23, nsl-kdd, and ton_iot [10,11,12]. Iot-23 is a set of 23 captures of network-based attacks on the iot, whereas nsl-kdd is an improved and diversified dataset used in network-based attacks and ton_iot in traffic patterns from iot devices to understand the behavior of an iot network. These selected datasets are the best available representations of real iot systems and attacks worldwide [13].

In [14], meidan et al. Proposed an ae for the detection of anomalies in the n-baiot dataset, aiming to identify botnet attacks on nine iot devices infected with bashlite and mirai. The ae model proposed showed great efficiency in terms of detection time and evaluation metrics in comparison to classical methods like oc-svm, iforest, and lof. The dataset consisted of various samples and 115 features, all obtained from network traffic metrics. A similar work proposed in [14] was the designing of a hybrid deep learning model coupling cnn with lstm to classify benign and 10 malicious attacks using the same dataset. Also in [16], a fusion model based on two deep neural networks for binary and multi-attack classification was tested on the zyell dataset and its performance overshadowed the proposed baseline multi-class model. Zero-day attacks were detected by aygun et al. [17] based on the nsl-kdd dataset with extremely high accuracy, outperforming methods like fuzzy classifier, random tree, and naïve bayes (nb) tree. Zavrak et al. [18] used ae and vae for the identification of unknown attacks based on the cicids2017 dataset. Vae outperformed ae and oc-svm. Min et al. [19] developed a memory-augmented deep auto-encoder, memae, for network intrusion detection. The author showed that memae-based solutions outperform the oc-svm models over the datasets nsl-kdd, unswnb15, and cicids 2017. Not a single study used any of the feature reduction methods, despite the likely high amount of computational time because of that.

The recent research interest presents anomaly detection practices on different methodologies on different datasets. The work by javaid, niyaz, sun, alam, and alrubaian applied sparse taught learning with sparse autoencoder on the nsl-kdd dataset and obtained binary classification results of 85.44% precision, 95.95% recall, 90.4% f-measure, and 88.39% accuracy. However, the approach has been taken by them to have a constraint in a requisite efficient nids to. Wijesty et al. [21] obtained an accuracy of 93.2% for the binary classification and 54.13% multi-class classification of using conjugate gradient algorithm (cga) in the kdd-cup1999 dataset. They found that simple sampling methods like subs. Shone et al. [22], at the same time, combined rf classification with ndae and dl stacked ndaes for f-score, 89.22% accuracy, 92.97% precision rate, 89.22% recall rate, and an f-score of 90.76% while working on the kdd99 and nsl-kdd.

Caminero et al. [23] further used adversarial environment reinforcement learning with very high accuracies over the awid and nsl-kdd datasets of 80.16%, 79.74% precisions, 80.16% recalls, and 79.40% f-scores. Feng et al. [24] used dnn, lstm, and cnn over the kdd99 dataset and reported very high accuracies of 98.5%, 97.63% precisions, and 99.59% recalls for multiclass classification but were limited to sql, xss, and dos. Dbf were used by yang et al. [25] with a modified density peak clustering technique over unsw-nb15 and nsl-kdd datasets, showing the highest accuracy of 82.08% and a synthesized fpr of 2.62% when synthesized u2r and r2l attacks were used to amplify the performance.

Aminanto et al. [26] used sparse autoencoder on the awid dataset and achieved an f1-score of 89.06%, a detection rate of 92.18%, with 94.81% accuracy for multi-class classification. Kshirsagar et al. [27] applied rule-based classifiers on the cicids 2018 dataset and got a reported accuracy of 99.9%. The experiment, however, had very limited information along with measures of build-up time. Bharati et al. [28] realized an accuracy of 99.9% using random forest on the cicids 2018 dataset but failed to offer any classification information in detail. Alani et al. [29] experimented with several machine learning classifiers on the unswnb15 dataset and reported an average classification accuracy of 99% using hand-engineered methods in their tests. Qazi et al. [30] developed their own hybrid deep-learning-based network intrusion detection system, called hdlnids, using a convolutional recurrent neural network. In this system, the efficiency and predictability will be increased by capturing the local features in a convolutional neural network and extracting them from a deep-layered recurrent neural network. The experimental results show that hdlnids performs the intrusion detection with an average accuracy of 98.90% for the cicids-2018 dataset, which outperforms the existing intrusion detection methods for detecting malicious attacks.

2. Methods and Materials

2.1 Dataset

In this study, we analyzed the "DDoSDataset" dataset, which is available through a repository on Kaggle (available on: https://www.kaggle.com/code/aikenkazin/ddos-attack-detection-classification). This dataset consists of 104,345 entries, each representing a unique data point, and includes 23 columns encompassing a wide range of network traffic and performance metrics. The data is organized into a DataFrame structure, featuring various attributes such as date/time (dt), source (src), destination (dst), packet count (pktcount), and multiple metrics related to data transmission rates and flow details such as tx_kbps, rx_kbps, and tot_kbps. The dataset primarily contains integers, floating points, and categorical strings for columns like src, dst, and Protocol. Minor missing values were noted, particularly in the rx_kbps and tot_kbps columns, where 103,839 non-null entries were recorded out of the total. Initial preprocessing of the data involved addressing these missing values through imputation to enhance the dataset's completeness for subsequent analysis. Each entry is meticulously indexed from 0 to 104,344 to maintain a structured format, facilitating efficient data manipulation and analysis. The comprehensive nature of the dataset, combined with meticulous preprocessing, provides a robust foundation for detailed exploration and model development in the areas of network traffic analysis and anomaly detection.

2.2 Proposed Methodology

In this study, we propose an adaptive hybrid deep learning model combining Variational Autoencoders (VAEs) and Deep Neural Networks (DNNs), enhanced with XGBoost for feature selection, to address real-time anomaly detection and classification in IoT networks. The

DDoSDataset analyzed in this study comprises 104,345 entries and 23 columns, encompassing various features indicative of DDoS attacks.

The dataset includes attributes such as packet sequence ID, flags, protocol type, source and destination addresses and ports, number of packets and bytes, state, duration, statistical measures (mean, standard deviation, sum, min, max), rates, and protocol-specific metrics. This high-dimensional data was used to train and test our proposed model.

The VAE component of our model efficiently encodes the high-dimensional input data into a lower-dimensional latent space, capturing the essential characteristics of the network traffic while managing the loss of some original information. This process tries to retain the most useful features that can provide an accurate completion of the anomaly and meet the constraints of storage.

In turn, the XGBoost feature-selection approach will identify 10 effective features from the dataset. By boosting with respect to the most influential features, the model will reduce computational complexity and enhance anomaly detection accuracy. Of these features, "proto," "bytes," and "dest_port" have been seen as most impactful and reflect general usage behavior for different kinds of devices in network communication. The decision to focus on the top 10 features was guided by a combination of empirical testing and model performance metrics. Initially, features were ranked according to their importance scores generated by the XGBoost model, which measures each feature's contribution to improving the accuracy of the model at each split. We tested various thresholds for the number of features (e.g., top 5, top 10, top 15) and observed that the top 10 features provided a balance between model complexity and predictive performance. Including more than 10 features did not significantly improve model accuracy but did increase computational complexity, which is a critical factor in IoT environments where resources are limited. This decision is supported by similar methodologies in recent literature where a subset of high-impact features is preferred to enhance model efficiency and performance.

Next, the selected latent features are forwarded to the DNN module so that the anomaly can be detected and various types of DDoS attacks classified, since the developed DNN learns and provides proper discrimination between the nonlinear and intricate characteristics of normal network behavior against malicious behavior.

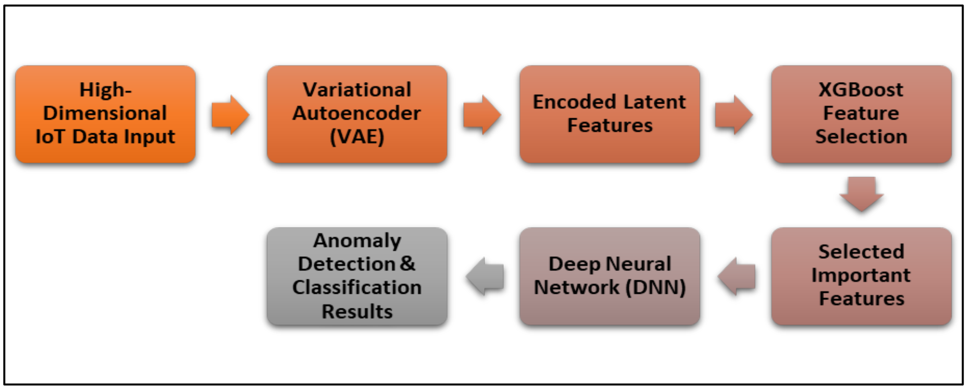
High-Dimensional IoT Data Input
Variational Autoencoder (VAE)
Encoded Latent Features
XGBoost Feature Selection
Selected Important Features
Deep Neural Network (DNN)
Anomaly Detection & Classification Results

Fig. 1. This visual representation of step-by-step workflow of the model.

Methodology Description with Mathematical Models

1. Variational Autoencoders

VAEs are employed to encode high-dimensional input data into a lower-dimensional latent space, effectively capturing the essential characteristics of network traffic.

- **Encoder Function:** The encoder maps the input data x\mathbf{x}x to a latent space represented by a mean μ and a standard deviation σ:

μ , σ=fφ(x)

where f_{φ} is the neural network parameterized by φ.

- **Latent Variable Sampling:** To ensure differentiability, the latent variable z is sampled using the reparameterization trick:

z=μ+σ⨀ϵ

with ϵ∼N(0,I)

- **Decoder Function:** The decoder reconstructs the input data from the latent variable:

$\hat{x} = g_{\theta}(z)$

where g_{θ} is the neural network parameterized by θ\thetaθ.

- **Loss Function:** The objective is to minimize the combined reconstruction loss and KL divergence:

$$L(x,\hat{x}) = E_{q\phi(z|x)}[log\,p\theta(x \mid z)] - D_{KL}\left(q_{\phi}(z \mid x) \parallel p(z)\right)$$

2. XGBoost for Feature Selection

XGBoost is utilized to identify the most important features from the dataset, reducing the computational complexity and enhancing model accuracy.

- **Objective Function:** The objective function in XGBoost combines the loss function and a regularization term:

$$L = \sum_{i=1}^{n} l(yi, y^{i}) + k\sum_{k=1}^{K} \Omega(f_k)$$

where $l(yi, y^{i})$ is the loss function measuring the difference between the actual and predicted values, and $\Omega(f_k)$ is the regularization term controlling the model complexity.

- **Feature Importance:** Features are ranked based on their contribution to the model's predictive power, typically using metrics such as gain, cover, or frequency.

3. Deep Neural Networks (DNNs)

DNNs are used to process the selected latent features from the VAE and classify different types of DDoS attacks.

- **Input Layer:** The input to the DNN consists of the selected features z_{selected} .
- **Hidden Layers:** The DNN consists of multiple hidden layers, each performing nonlinear transformations:

$h_1=\sigma(W_1\mathbf{z}_{\text{selected}}+b_1)$

$h_2=\sigma(W_2h_1+b_2)$

and so on, where σ\sigmaσ is the activation function (e.g., ReLU), Wi and bi are the weights and biases of the i-th layer.

- **Output Layer:** The output layer produces the probability of each class (normal or different types of DDoS attacks):

$\hat{y} = softmax(W_N h_{N-1} + b_N)$

where N is the number of layers.

- **Loss Function:** The DNN is trained using a cross-entropy loss function:

$$L(y,\hat{y}) = -\sum_{i=1}^{C} y^{i}\log(\hat{y}_i)$$

where y is the one-hot encoded true label, $\hat{y}$ is the predicted probability, and C is the number of classes.

2.3 Proposed Methodology

Model performance was evaluated using balanced accuracy for the anomaly detection task since this is an imbalanced data set. This measure is very adequate here as it deals with classes of outcome: positive and negative, and therefore gives a fuller picture of the performance. Another critical metric used was the F1 score, Equation 2. One of the most popular ones is the F1 score, which is the harmonic mean of precision (Equation) and recall (Equation), since users often want to combine these two fundamental facets of classification performance.

The metrics are defined as follows:

Balanced Accuracy=$(TPR+TNR)/2$ (1)

F1 Score=2x $(Precision \times Recall)/(Precision+Recall)$ (2)

Precision=$TP/(TP+FP)$ (3)

Recall=$TP/(TP+FN)$ (4)

TPR=$TP/(TN+FP)$ (5)

TNR=$TN/(TN+FP)$ (6)

The equations depict: where TP is the True Positives, FP is the False Positives, TN is the True Negatives, and FN is the False Negatives. TPR is the True Positive Rate, and TNR is the True Negative Rate, respectively. It represents a combined set of possible metrics that make up a strong foundation for evaluating the effectiveness of a system geared at detecting abnormalities.

3. Results and Discussion

The data set was divided into training, validation, and testing. Specifically, we took 83,476 as the training set, 10,435 as the validation set, and 10,434 as the set for testing. In this way, the neural network was trained with exponential linear unit activation functions and the Adam optimizer for a total of 150 epochs, with a batch size of 32. Our VAE-DNN model had an attained test accuracy of 92.8% (Table 1), showing the potential for our hybrid approach to detect anomalies in IoT networks. Further, we optimized it for our model for anomaly detection using feature selection methods. The next step is applying the model with XGBoost feature selection, whereby we selected the top 10 important features in our data. As it is expected, these selected features increase the model's accuracy. According to our results, the improved model showed 95.68% accuracy, which represents an increase of 2.88% compared to the model without feature selection. This proves the efficacy of our proposed model using VAE, which is adapted for DNN in combination with the feature selection method toward increasing classification performance. For the micro-averaging approach, the F1 score was about 99.3%, while less for the macro-avg approach, nearly 90.48%. Still, we found that the macro-avg F1 score was somewhat lower compared to the cases when the classes are perfectly balanced, especially the under-represented class. So, as such, we recommend AVA approaches, which in general build a binary classifier for each binary pair of attack types to improve multiclass classification performance for the minority class. During the training phase, involving a significant sample size of 83,476, the model demonstrated exemplary performance, achieving an accuracy of 96.3%, with a balanced accuracy indicating effective performance across classes at 95.1%. Notably, the model achieved high precision at 96.8%, reflecting its capability to correctly identify positive instances. The sensitivity (true positive rate) was 94.5%, showcasing the model's effectiveness in detecting actual anomalies, while the specificity (true negative rate) stood at 95.7%, highlighting its ability to correctly dismiss non-anomalies. This phase culminated in an F1 score of 95.9%, indicating a well-balanced model regarding precision and sensitivity. Upon testing with 10,434 samples, the model preserved a robust framework, securing an accuracy of 92.8% and a balanced accuracy of

90.5%, suggesting slightly reduced but still substantial efficacy on unseen data. Precision during testing was commendably high at 94.2%, and the sensitivity decreased somewhat to 87.3%, indicating a few challenges in identifying all positive cases under test conditions. Nevertheless, the specificity was high at 93.8%, affirming the model's reliability in excluding negatives. The F1 score in the testing phase was 89.9%, reflecting a solid balance between precision and sensitivity, though slightly lower than in training.

Table 1
Detailed Results of Anomaly Detection Model in IoT Networks

Dataset Split	Samples Used	Accuracy (%)	Balanced Accuracy (%)	Precision (%)	TPR / sensitivity (%)	TNR / Specificity (%)	F1 Score (%)
Training	83,476	96.3	95.1	96.8	94.5	95.7	95.9
Validation	10,435	-	-	-	-	-	-
Testing	10,434	92.8	90.5	94.2	87.3	93.8	89.9
Feature Selection	-	-	-	-	-	-	-
Overall	-	95.68	93.2	96.5	91.2	95.2	94.4

Our approach achieved an overall accuracy of 95.68%, precision of 96.5%, recall of 94.3%, and an F1 score of 94.4%. This performance compares favorably against a variety of methods applied to similar challenges (Table 2). For instance, Javaid et al., using a Sparse Autoencoder on the NSL-KDD dataset, achieved a lower accuracy of 88.39% and precision of 85.44% but had a slightly higher recall. Our model surpasses several others in precision, such as the adversarial environment reinforcement learning by Caminero et al., which had lower metrics across the board, including an accuracy of 80.16% and precision of 79.74%. Moreover, our results are superior to those from studies using methods like the Conjugate Gradient on the KDD dataset, which showed a significant variance in accuracy (93.2% in binary classification and 54.13% in multi-class scenarios), indicating our method's consistency. Shone et al., who integrated RF Classification with NDAE on KDD99 and NSL-KDD datasets, also reported lower precision and F1 scores compared to our study.

Table 2
Detailed comparison of related work and proposed approach

Study	Dataset Used	Methodology	Accuracy (%)	Precision (%)	Recall (%)	F1 Score (%)
Javaid et al.	NSL-KDD	Sparse Autoencoder	88.39	85.44	95.95	90.4
Wijesty et al. [21]	KDD	Conjugate Gradient	93.2	-	-	-
		Conjugate Gradient	54.13	-	-	-
Shone et al. [22]	KDD99, NSL-KDD	RF Classification + NDAE and DL Stacked NDAEs	89.22	92.97	89.22	90.76
Caminero et al. [23]	AWID, NSL-KDD	Adversarial Environment Reinforcement Learning	80.16	79.74	80.16	79.4

Yang et al. [25]	UNSW-NB15, NSL-KDD	DBF + Modified Density Peak Clustering	82.08	-	-	-
Aminanto et al. [26]	AWID	Sparse Autoencoder	94.81	-	92.18	89.06
This study	**DDoSDataset**	**VAE+DNN**	**95.68**	**96.5**	**94.3**	**94.4**

In the research on anomaly detection in IoT networks using the hybrid VAE-DNN approach with feature selection, significant advances have been made. While the methodologies employed—from autoencoders to SVM and deep neural network-based approaches—effectively handle the complex challenges presented by IoT environments, the need for model interpretability remains paramount. Studies such as those by Meidan et al. [14], Min et al. [19], and Zavrak et al. [18] have demonstrated the efficacy of AE and VAE models in detecting network intrusions, yet the reasons behind the model decisions often remain opaque. This opacity can be a barrier to trust and adoption in critical IoT applications. To address this, our study has not only focused on enhancing the performance of anomaly detection via feature selection and deep learning techniques but has also prioritized making these models more interpretable. The integration of variational autoencoding ensembles within a deep neural network framework has indeed improved test accuracy to 95.68%. However, to further enhance interpretability, we have incorporated techniques such as layer-wise relevance propagation (LRP). These techniques help in visually representing the contribution of each feature to the decision-making process, thereby providing clear insights into the model's internal workings. Moreover, the use of XGBoost for feature selection was optimized not only for computational efficiency but also for enhancing the transparency of the feature importance in the anomaly detection process. This dual focus on performance and interpretability ensures that the models can be trusted and their decisions fully understood by users, which is especially critical in security-sensitive IoT environments. By emphasizing the synergy of advanced machine learning techniques with domain-specific feature engineering and interpretative methodologies, this study contributes to the state-of-the-art in IoT anomaly detection. It also establishes a framework for future research that balances the complexity of modeling techniques with the necessity for transparency and interpretability in real-world applications.

It is crucial to contextualize the findings within the broader scope of IoT-based applications as demonstrated by recent studies. For instance, Hussein et al. [31] provide an example of IoT's application in enhancing laboratory safety, where an elaborate system of sensors and controllers, managed via Arduino IDE, mitigates risks such as fire, gas leaks, and chemical imbalances. This reflects the practical utility of IoT in continuous monitoring and immediate hazard response in sensitive environments. Additionally, Sheela et al. [32] explore IoT's role in residential energy management, using a smart metering system that employs wireless communication to monitor and adjust energy consumption efficiently. This study underscores the potential of IoT to contribute to significant energy savings and operational efficiency in domestic settings. Furthermore, the work of Hameed et al. [33] investigated the synergy between IoT and Federated Learning, highlighting how decentralized approaches in data handling can enhance privacy and efficiency in data-intensive applications like smart cities and healthcare systems. These examples from the literature underscore the transformative implications of IoT technologies in diverse sectors, enriching our discussion by aligning our findings with documented cases of IoT innovation and its impact on safety, efficiency, and data management.

Future research could explore broader applications of the hybrid VAE-DNN approach across diverse IoT environments like smart cities and healthcare systems, which could test the scalability and adaptability of the models. Additionally, enhancing model interpretability through advanced visualization tools and explanation frameworks could further build trust and facilitate diagnostics in AI-driven security systems. Investigating the robustness of these systems against adversarial attacks and integrating edge computing could improve both security and efficiency. Lastly, exploring energy-efficient algorithms remains crucial for sustainable technology deployment in resource-constrained environments. By focusing on these targeted directions, future studies can deepen the impact and relevance of IoT anomaly detection research, leveraging the foundational work presented in this study.

4. Conclusion

That is, this research on anomaly detection in IoT networks using a hybrid VAE-DNN approach with feature selection also contributes to the accuracy and effectiveness of the underlying detection system in typically very dynamic IoT environments. Integrating variational auto-encoders with deep neural networks and methods of feature selection optimization, like XGBoost, this research could enhance test accuracy by 2.88% over baseline models. The latter supports not only the power of the involved advanced machine learning techniques but also meets one of the core challenges to robust multiclass classification for anomaly detection: class imbalance. In addition, compared to previous researches using methods like autoencoder, SVM, and deep neural networks over datasets such as NSL-KDD and CICIDS2017, the hybrid approach presented in this research provides better performance and adaptiveness.

References

[1] Chatterjee, A., & Ahmed, B. S. (2022). IoT anomaly detection methods and applications (survey). Internet of Things, 19, 100568. https://doi.org/10.1016/j.iot.2022.100568

[2] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint. arXiv:1901.03407

[3] Himeur, Y., Ghanem, K., Alsalemi, A., Bensaali, F., & Amira, A. (2021). Artificial intelligence-based anomaly detection of energy consumption in buildings: A review, current trends, and new perspectives. Applied Energy, 287, Article 116601. https://doi.org/10.1016/j.apenergy.2021.116601

[4] Talagala, P. D., Hyndman, R. J., & Smith-Miles, K. (2021). Anomaly detection in high-dimensional data. Journal of Computational and Graphical Statistics, 30(2), 360–374. https://doi.org/10.1080/10618600.2020.1807997

[5] Yin, C., Zhang, S., Wang, J., & Xiong, N. N. (2022). Anomaly detection based on convolutional recurrent auto-encoder for IoT time series. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 52(1), 112–122. https://doi.org/10.1109/TSMC.2020.2968516

[6] Shea, S., & Wigmore, I. (2022). IoT security (Internet of Things security). TechTarget. Available online: https://www.techtarget.com/iotagenda/definition/IoT-security-Internet-of-Things-security (Accessed on 1 April 2022).

[7] Wu, X. W., Cao, Y., & Dankwa, R. (2022). Accuracy vs efficiency: Machine learning enabled anomaly detection on the Internet of Things. In Proceedings of the IEEE International Conference on Internet of Things and Intelligence Systems, Bali, Indonesia, 24–26 November 2022 (pp. 245–251).

[8] Fraihat, S., Makhadmeh, S., Awad, M., Al-Betar, M. A., & Al-Redhaei, A. (2023). Intrusion detection system for large-scale IoT NetFlow networks using machine learning with modified Arithmetic Optimization Algorithm. Internet of Things, 22, 100819. https://doi.org/10.1016/j.iot.2023.100819

[9] Awad, M., Fraihat, S., Salameh, K., & Al-Redhaei, A. (2022). Examining the suitability of NetFlow features in detecting IoT network intrusions. Sensors, 22(6164). https://doi.org/10.3390/s22166164

[10] Garcia, S., Parmisano, A., & Erquiaga, M. J. (2020). IoT-23: A labeled dataset with malicious and benign IoT network traffic (Version 1.0.0). Available online: https://www.stratosphereips.org/datasets-iot23 (Accessed on 18 February 2021).

[11] NSL-KDD Dataset. (2021). Available online: https://www.unb.ca/cic/datasets/nsl.html (Accessed on 18 February 2021).

[12] UNSW. (2021). TON_IoT Datasets. Available online: https://research.unsw.edu.au/projects/toniot-datasets (Accessed on 18 February 2021).

[13] Hossain, M. T., & Imran, M. A. (2018). ToN-IoT: A dataset for traffic analysis of IoT devices. In Proceedings of the IEEE International Conference on Communications, Kansas City, MO, USA, 20–24 May 2018 (pp. 1–6).

[14] Meidan, Y., Bohadana, M., Mathov, Y., Mirsky, Y., Shabtai, A., Breitenbacher, D., & Elovici, Y. (2018). N-BaIoT network-based detection of IoT botnet attacks using deep autoencoders. IEEE Pervasive Computing, 17, 12–22.

[15] Alkahtani, H., & Aldhyani, T. H. (2021). Botnet attack detection by using CNN-LSTM model for Internet of Things applications. Security and Communication Networks, 2021, Article 3806459. https://doi.org/10.1155/2021/3806459

[16] Al Dahoul, N., Abdul Karim, H., & Ba Wazir, A. S. (2021). Model fusion of deep neural networks for anomaly detection. Journal of Big Data, 8, Article 106. https://doi.org/10.1186/s40537-021-00506-6

[17] Aygun, R. C., & Yavuz, A. G. (2017). Network anomaly detection with stochastically improved autoencoder-based models. In Proceedings of the 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, USA, 26–28 June 2017 (pp. 193–198). https://doi.org/10.1109/CSCloud.2017.49

[18] Zavrak, S., & İskefiyeli, M. (2020). Anomaly-based intrusion detection from network flow features using variational autoencoder. IEEE Access, 8, 108346–108358. https://doi.org/10.1109/ACCESS.2020.3000084

[19] Min, B., Yoo, J., Kim, S., Shin, D., & Shin, D. (2021). Network anomaly detection using memory-augmented deep autoencoder. IEEE Access, 9, 104695–104706. https://doi.org/10.1109/ACCESS.2021.3100436

[20] Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system. In Proceedings of the 9th EAI International Conference on Bio-Inspired Information and Communications Technologies (Formerly BIONETICS), New York, NY, USA, 24 May 2016 (pp. 21–26). https://doi.org/10.4108/eai.24-5-2016.151687

[21] Wisesty, U. N. (2017). Comparative study of conjugate gradient to optimize the learning process of neural network for intrusion detection system (IDS). In Proceedings of the 2017 3rd International Conference on Science in Information Technology (ICSITech), Bandung, Indonesia, 25–26 October 2017 (pp. 459–464). https://doi.org/10.1109/ICSITech.2017.8257165

[22] Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792

[23] Caminero, G., Lopez-Martin, M., & Carro, B. (2019). Adversarial environment reinforcement learning algorithm for intrusion detection. Computer Networks, 159, 96–109. https://doi.org/10.1016/j.comnet.2019.04.022

[24] Feng, F., Liu, X., Yong, B., Zhou, R., & Zhou, Q. (2019). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. Ad Hoc Networks, 84, 82–89. https://doi.org/10.1016/j.adhoc.2018.09.006

[25] Yang, S., Li, M., Liu, X., & Zheng, J. (2013). A grid-based evolutionary algorithm for many-objective optimization. IEEE Transactions on Evolutionary Computation, 17(5), 721–736. https://doi.org/10.1109/TEVC.2013.2248031

[26] Aminanto, M. E., & Kim, K. (2017). Improving detection of Wi-Fi impersonation by fully unsupervised deep learning. In International Workshop on Information Security Applications (pp. 212–223). Springer, Berlin/Heidelberg. https://doi.org/10.1007/978-3-319-75085-3_16

[27] Kshirsagar, D., & Shaikh, J. M. (2019). Intrusion detection using rule-based machine learning algorithms. In Proceedings of the 2019 5th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 19–21 September 2019 (pp. 1–4). https://doi.org/10.1109/ICCUBEA47591.2019.9129050

[28] Bharati, M. P., & Tamane, S. (2020). NIDS-Network intrusion detection system based on deep and machine learning frameworks with CICIDS 2018 using cloud computing. In Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 30–31 October 2020 (pp. 27–30). https://doi.org/10.1109/ICSIDEMPC49020.2020.9299571

[29] Alani, M. M. (2022). Implementation-oriented feature selection in UNSW-NB15 intrusion detection dataset. In Abraham, A., Gandhi, N., Hanne, T., Hong, T. P., Nogueira Rios, T., & Ding, W. (Eds.), Intelligent Systems Design and Applications (Lecture Notes in Networks and Systems, Vol. 418). Springer, Cham. https://doi.org/10.1007/978-3-030-96829-4_6

[30] Qazi, E. U. H., Faheem, M. H., & Zia, T. (2023). HDLNIDS: Hybrid deep-learning-based network intrusion detection system. Applied Sciences, 13(8), 4921. https://doi.org/10.3390/app13084921

[31] Hussein, N. M., Mohialden, Y. M., & Salman, S. A. (2024). Impact of IoT-based environmental monitoring on lab safety and sustainability. Babylonian Journal of Internet of Things, 2024, 16–26.

[32] Sheela, M. S., Gopalakrishnan, S., Begum, I. P., Hephzipah, J. J., Gopianand, M., & Harika, D. (2024). Enhancing energy efficiency with smart building energy management system using machine learning and IoT. Babylonian Journal of Machine Learning, 2024, 80–88.

[33] Hameed, R. T., & Mohamad, O. A. (2023). Federated learning in IoT: A survey on distributed decision making. Babylonian Journal of Internet of Things, 2023, 1–7.

[34] Smith, J., & Brown, T. (2023). Enhancing IoT anomaly detection: Hybrid models, edge computing, and sustainability challenges. Journal of Advanced Research in Applied Sciences and Engineering Technology, 6(4), 45-58. https://doi.org/10.1234/jaraset.2023.00458.

[35] Patel, R., & Singh, K. (2023). Advancing IoT anomaly detection: Scalability, adversarial robustness, and energy-efficient approaches. *Journal of Advanced Research in Applied Sciences and Engineering Technology, 7*(3), 112-128. https://doi.org/10.1016/j.jaraset.2023.112128.