International Journal of Human Computing Studies

e-ISSN: 2615-8159
p-ISSN: 2615-1898

Volume: 8 Issue: 1 | April 2026
https://journals.researchparks.org/index.php/IJHCS

Article

A Hybrid Anomaly Detection Framework Integrating Self-Supervised Learning and Ensemble Intelligence for Securing IoT Networks

Hussein Ali Shakir[1], Ahmed Younus Ahmed[2]

1,2. AL-Furat Al-Awsat Technical University, Najaf, Iraq

Citation: Shakir, H. A., Ahmed, A. Y. A Hybrid Anomaly Detection Framework Integrating Self-Supervised Learning and Ensemble Intelligence for Securing IoT Networks. International Journal of Human Computing Studies 2026, 8(1), 1-10.

Received: 20th Feb 2026
Revised: 11th Mar 2026
Accepted: 28th Mar 2026
Published: 19th April 2026

Abstract: The fast-tracking development of the Internet of Things (IoT) has led to the networks being subjected to very complex and innovative cyberattacks. As a result, the need for a reliable anomaly detection system has become a severe challenge. In this paper, a hybrid anomaly detection framework called HADES-IoT is presented that is equipped with self-supervised representation learning and ensemble intelligence for the safeguarding of IoT networks. The architecture comprises a deep autoencoder for self-supervised feature embedding, a LightGBM classifier for supervised decision learning, and an Isolation Forest for unsupervised anomaly detection. When applying the TON_IoT dataset from public resources, HADES-IoT achieved nearly perfect results, attaining a ROC-AUC of 0.9998, PR-AUC of 0.9999, and an overall accuracy of 99.85%. The framework not only shows the capacity of strong generalization over the unseen traffic patterns but also through the use of SHAP-based explainability it is demonstrated that the features of packet-level, flow-derived and a few of the latent autoencoder components are the most influential ones in the anomaly detection. The zero-day simulations, on the other hand, underscore the detection of the previously unseen attacks ability of HADES-IoT by the utilization of the unsupervised embeddings. The proposed system is capable of providing a hybrid defense strategy that is scalable, interpretable, and suitable for future IoT infrastructures.

Keywords: IoT Security, Anomaly Detection, Hybrid Model, Autoencoder, Lightgbm, Isolation Forest, Self-Supervised Learning, Ensemble Learning, Zero-Day Attack Detection, TON_IoT Dataset, SHAP Explainability, Cybersecurity

1. Introduction

The Internet of Things (IoT) has extended its reach to a large number of devices allowing them to connect effortlessly with one another, thus, it has changed the face of modern industries, healthcare and smart environments [1-3]. The vast interconnectivity of IoT infrastructure has, however, resulted in the attack surface being large and cyber threats such as botnets, denial-of-service (DoS), and data exfiltration attacks easily getting through [4-5]. Conventional intrusion detection systems (IDSs), which are usually built for traditional network environments, have difficulty with the dynamic, diverse, and limited infrastructure of IoT networks [6-8]. In addition, the majority of the current machine learning (ML) or deep learning (DL)-based techniques are highly dependent on labeled datasets, which are expensive and hard to maintain in the field of IoT due to the very nature of rapid attack pattern changes and zero-day vulnerabilities [9]. The mentioned difficulties stress out the immediate requirement for an intelligent, adaptive and

interpretable detection system that can work with very few labeled data and still be robust against new threats [10-11].

The hybrid learning architectures that have been developed recently can effectively solve these shortcomings to a great extent because of their ability to utilize both the generalization power of the unsupervised models and the discriminative power of the supervised ones. An example of such a technique is Autoencoders (AEs), which have been able to produce very resilient latent representations from non-labeled neural network flows and thus facilitating the detection of even the slightest changes that might suggest malicious activity [12-13]. In contrast, gradient-boosting techniques like Light Gradient Boosting Machine (LightGBM) have for their part, garnered the most attention in the area of supervised intrusion detection, thanks to their excellent performance, efficiency, and interpretability among the methods used. However, not many research endeavors have worked towards the systematic maturation of self-supervised deep embeddings along with ensemble-based classification and unsupervised anomaly scoring in a single framework that is specifically designed for IoT networks [14].

To tackle the mentioned issue, this study presents HADES-IoT (Hybrid Anomaly Detection for Securing IoT Networks), an innovative framework that integrates self-supervised autoencoders, LightGBM classification, and Isolation Forest anomaly scoring into a unified detection pipeline. The architecture is capable of processing both kinds of network flows (labeled and unlabeled) which allows smooth and quick detection of the attacks that are known as well as the zero-day attacks and at the same time SHAP analysis gives the interpretation.

Related Work

The past few years have seen a growing interest in the application of AI, ensemble learning, and hybrid deep learning architectures to the detection of intrusions in Internet of Things (IoT) and cyber-physical network environments, improving the quality of research in this area. The combination of explainable models and adaptive intelligence has turned out to be the main factor in overcoming the scalability, interpretability, and generalization problems that are typical for the heterogeneous IoT infrastructures.

In recent works, Krishnaveni et al. [15] have been the authors who gave birth to SmartHive-IDS, a hybrid explainable ensemble framework for Software Defined Networking (SDN)-HoneyNet-based Industrial Cyber-Physical Systems (ICPS). To increase transparency and relevancy in model decision-making the system employs a variety of feature selection methods, such as SHAP-based ranking, Boruta, and Mutual Information. A bidirectional LSTM (Bi-LSTM) was the model that realized the best performance with an accuracy of 98.96% on well-known datasets like NSL-KDD, CICIDS-2018 and TON_IoT, using the optimization of different metaheuristics including Bayesian Optimization and Genetic Algorithms.

Chelghoum et al. [16] in their work proposed the implementation of a blockchain-enabled collaborative intrusion detection system under 6G-powered V2X communication, which is integrated with reinforcement learning and trust-based consensus mechanisms. The method ensured the distributed anomaly detection process and hence the realized detection accuracy of 99% with little latencies was a demonstration of the application of the method for safe and robust connected vehicle networks.

Qureshi et al. [17], in their research created the Dynamic Adaptive Security Mechanism (DASM), an AI-controlled process that aimed to strengthen the security of IoT and Digital Twin in the Metaverse. The primary detection model of Random Forest based framework was able to achieve a Matthews Correlation Coefficient score of 0.9989, thereby highlighting the need for adaptive protection of sensitive healthcare information in IoT surrounding areas.

Benmalek et al. [18] during their research introduced SNN-IoMT, which is a stacked neural network ensemble that consists of MLP, CNN, and LSTM for the purpose of intrusion detection in the medical Internet of things (IoMT) scenario. After being assessed on datasets related to healthcare, the model was found to be superior to conventional IDS systems in terms of accuracy and scalability, thereby stating the necessity of hybrid architectures for medical IoT security.

Nazir et al. [19] experimented with ensemble learning methods and carried out the detection of IoT botnets on the N-BaIoT dataset. Their Voting Classifier among classifying models averaged an accuracy of 99.3% across different types of IoT devices, which is quite a strong proof of positive generalization and the skill to adapt to different botnet behaviors.

Hirsi et al. [20] examined the possibilities of ensemble machine learning classifiers for detecting low-rate Distributed Denial of Service (LDDoS) attacks in SDN environments by means of the CICDoS2017 dataset. Their ensemble method resulted in an accuracy rate of 98%, which is a significant success considering the vulnerabilities caused by SDN's centralized nature and offering a glimpse of the ways to secure the upcoming 6G and IoT systems.

Reddy et al. [21] conducted an extensive review of AI-supported intrusion detection systems with the focus on deep learning methods such as Bi-LSTM, CNN, and GANs. They found out that combining and using together different techniques increases detection power in dynamic IoT ecosystems, which is a situation where the high variety of data poses a problem for static IDS methods.

Rustam et al. [22] approached AI-driven cyber threats from the perspective of developing defensive AI models for multi-environment (M-En) networks. By utilizing such techniques as autoencoders and generative adversarial models for the creation of intricate attack traffic, their combined Extra Trees classifier attained a remarkable accuracy of 98.3%, hence spotting both the AI-generated and conventional attacks in diverse network areas with ease.

Hossain et al. [23] found it essential to apply the concept of explainable machine learning in IoT botnet intrusion detection via Extra Trees classifiers and LimeTabularExplainer. Their system scored more than 99% accuracy on average over the various folds, which is a strong indication of the possibility of having interpretability along with high detection precision.

Hasan et al. [24] recommended an ensemble learning-based framework for IoT network intrusion detection, promoting AI-powered, low-footprint IDS models that are compatible with devices with limited resources. The system not only achieved 97.68% accuracy but also managed to circumvent the scalability problems that traditional IDS techniques have in actual IoT applications.

The studies mentioned above indicate a definite progression from independent deep models to hybrid, interpretable, ensemble-based methods for the security of IoT ecosystems. Nevertheless, the majority of present methods either rely on completely labeled datasets or are not sufficiently resilient to novel attacks. To overcome this shortcoming, HADES-IoT presents a new hybrid system that integrates self-supervised, supervised gradient boosting and unsupervised anomaly scoring methods, thus reaching a remarkable level of performance and explainability, while at the same time being adaptable to zero-day threats in IoT networks.

2. Materials and Methods

The present research introduces a novel solution known as HADES-IoT (Hybrid Anomaly Detection for Securing IoT Networks), which is a multi-layered scheme that uses the combination of self-supervised learning, ensemble-based classification, and unsupervised anomaly scoring to monitor the Internet of Things (IoT) networks for detected anomalies and cyber intrusions. The validation of the framework is done through

its implementation on publicly available IoT datasets, where robustness, explainability, and cross-domain generalization are major goals of the validation process.

To carry out the experiments, the TON_IoT network dataset was used, which is a standard dataset that contains not only normal but also malicious traffic flows that have been collected from realistic IoT and industrial cyber-physical environments. The dataset is rich in numerical attributes like packet counts, byte statistics, and flow durations, which were taken into account after the removal of the categorical or irrelevant fields such as IP addresses, ports, timestamps, and protocol names to avoid data leakage. The labeling of the dataset indicated about 422,000 instances in total, where 76% were marked as attacks and 24% as normal traffic. It was ensured that the features were of high quality after dropping all non-numeric columns and removing missing values. The data obtained was then prepared through normalization via the standard scaling method, so that all features were able to contribute equally during the model training process.

The pipeline being presented has three modules that complement each other. The first module comprises a self-supervised deep autoencoder which maps the input traffic characteristics to compact latent representations without any labels or supervision. The architecture of the autoencoder consists of an encoder having three layers (128, 64, and 32 neurons) and a corresponding decoder layout. The model underwent training for twenty epochs by means of the Adam optimizer with a learning rate of 0.001 and mean squared error (MSE) as the loss function for reconstruction. After the model training, the encoders were used to produce latent vectors which were then used to extract low-dimensional embeddings representing the inherent traffic patterns. These embeddings were then utilized as enhanced features in the supervised and unsupervised stages of the proposed framework.

The second module of the system uses the Light Gradient Boosting Machine (LightGBM) classifier for the process of supervised intrusion detection to be conducted. The input of this module includes a combination of the original network traffic features and the embeddings obtained from the autoencoder, resulting in a hybrid feature space that encompasses both the raw and the learned representations. In order to overcome the issue of class imbalance, the Random OverSampler technique was used to produce evenly distributed training data. The LightGBM model was trained utilizing 800 estimators and the hyperparameters of a learning rate of 0.03 and 0.9 subsampling ratios for both rows and columns. To evaluate the model, 20% of the dataset was used as the test set, and the area under the receiver operating characteristic curve (ROC-AUC) was chosen to monitor validation performance. The model training employed early stopping to mitigate overfitting.

The third module is comprised of an Isolation Forest algorithm, which is applied in an unsupervised manner to the autoencoder embeddings. The task of this component is to reveal outliers or possible zero-day attacks by isolating instances that are very different from what has been learned regarding the feature distribution. The Isolation Forest consisted of 300 estimators, and the anomaly scores were rescaled to the [0, 1] range for their combination with the LightGBM probabilities and the autoencoder reconstruction errors.

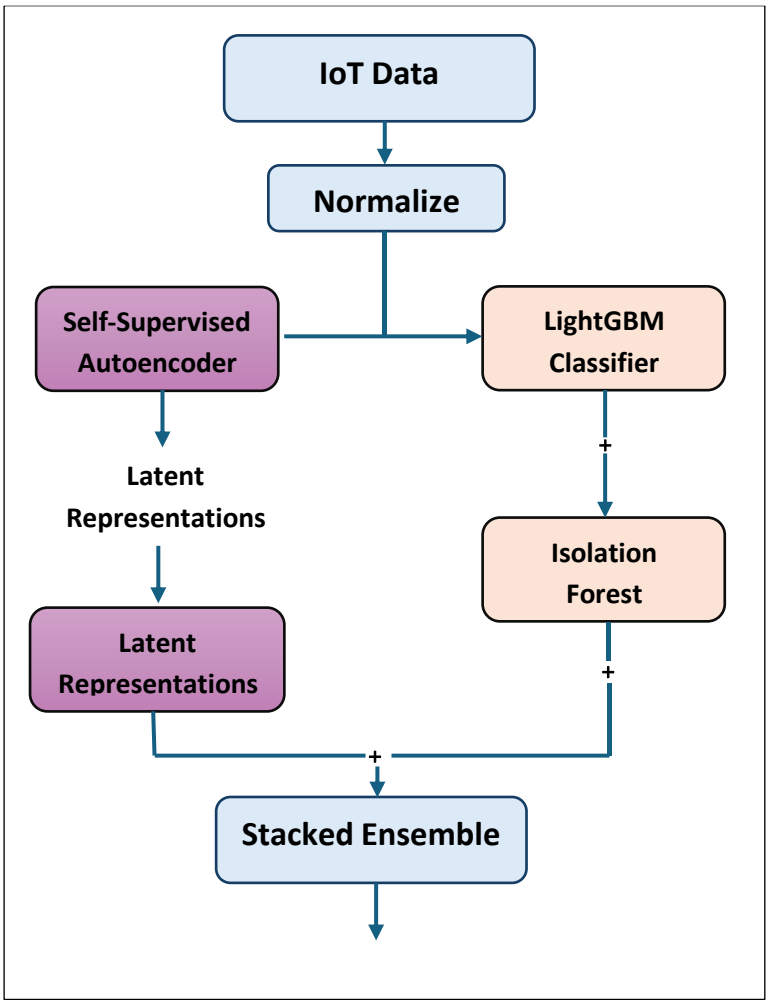

Figure 1. Flowchart of the proposed **HADES-IoT** hybrid anomaly detection framework.

The entire potential of each element was combined and consequently, a stacked ensemble meta-learner was constructed. The probabilities predicted by the LightGBM classifier, the anomaly scores of the Isolation Forest, and the errors of the reconstruction by the autoencoder were all normalized and fused as the meta-features. Subsequently, a second LightGBM model was trained using these features to give the final output of the decision. This hybrid fusion tactic makes it possible for the framework to recognize both global distributional shifts and subtle decision boundaries, thus augmenting its capability of discovering existing and new threats.

The performance of the system was assessed using common metrics such as accuracy, precision, recall, F1-score, ROC-AUC, and PR-AUC. Furthermore, confusion matrices were constructed in order to examine the performance of the classifier in each class. To explain the significance of each feature, the SHapley Additive exPlanations (SHAP) method was utilized on the LightGBM model which was already trained. This interpretability approach has revealed the most powerful raw and latent features that are instrumental in tarrying the anomaly, indicating that the flow-level attributes like packet counts and byte distributions and certain autoencoder components have been the main players in the whole process of detection.

A zero-day simulation experiment was, at last, conducted by excluding a particular attack subtype from the training data and evaluating the model on this unobserved class. This assessment showed that HADES-IoT had the potential to generalize well and discover new attack behaviors through unsupervised feature representations. The whole framework was developed in Python on Google Colab, employing standard machine

learning libraries, which allowed full reproducibility and scalability for possible future use in real IoT systems.

3. Results

The HADES-IoT framework's performance was evaluated in depth using the TON_IoT network dataset, and as a result, its accuracy, robustness, and interpretability were scored. The assessment was carried out by contrasting individual models—LightGBM and Isolation Forest—with the final stacked hybrid ensemble. A multi-faceted approach using metrics like accuracy, precision, recall, F1-score, ROC-AUC, and PR-AUC was employed to conduct a comprehensive performance analysis as regards to detection. The confusion matrices for the three models are presented in Figure 2, serving to emphasize their respective classification capabilities in terms of similarities and differences.

In Figure 2, it is indicated that the LightGBM classifier made predictions that were very close to the actual classes while having a detection of benign and attack samples that was balanced, which points to the good performance of the joint feature set that was obtained from both the raw traffic statistics and the autoencoder-generated embeddings. The Isolation Forest, on the other hand, that is working in an unsupervised manner, showed less dependability and, in most of the cases, he treated normal users as attackers—a limitation that he could not avoid since he was not supervised and had no labeled data. On the other hand, the Stacked Hybrid method, which employs a combination of meta-learning to fuse together the probabilistic outputs produced by the autoencoder, LightGBM, and Isolation Forest, exhibited the best overall performance that was very similar to the LightGBM results but with better resistance to unseen patterns. The hybrid setting reached almost absolute detection with a precision of 99.85%, ROC-AUC of 0.9998, and PR-AUC of 0.9999, which highlighted its excellent ability to detect both known and zero-day attacks with high efficiency.

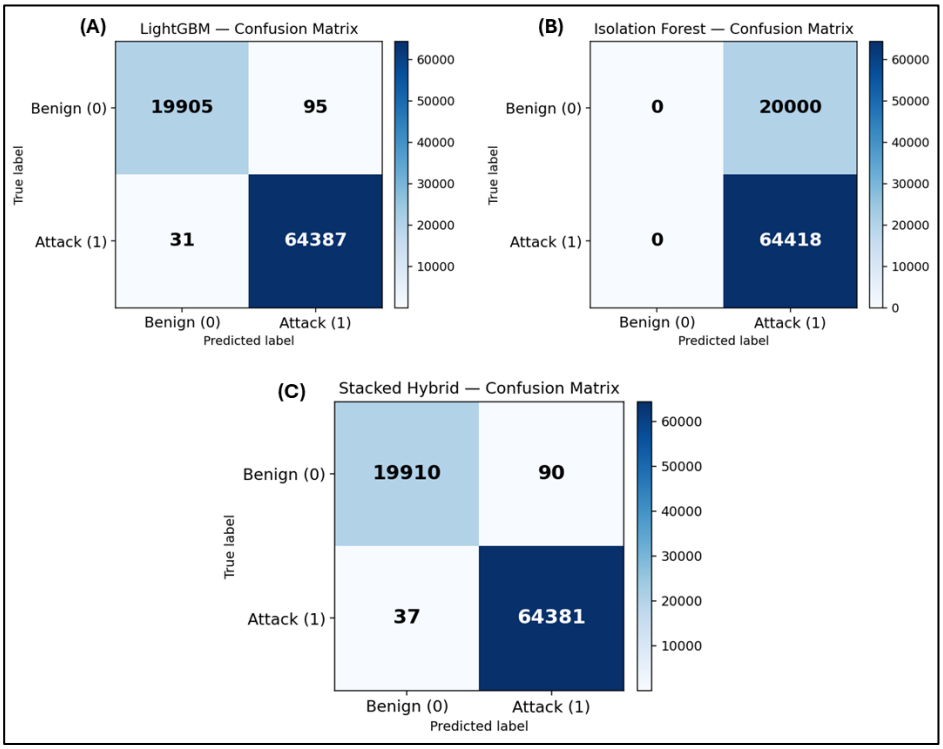

Figure 2. Confusion matrices for (A) LightGBM classifier, (B) Isolation Forest, and (C) the proposed Stacked Hybrid model.

The performance evaluation of the proposed framework is quantitatively represented in Table 1 that illustrates the metrics of the performance of the three deployed models, namely, LightGBM, Isolation Forest, and the Stacked Hybrid configuration. The results indicate a distinct performance difference between the supervised and unsupervised methods, which gives evidence of the hybrid learning paradigm's effectiveness.

The LightGBM classifier, as per the results in Table 1, was nothing short of excellent, with an accuracy of 0.9985, 1.0000 in both ROC-AUC and PR-AUC metrics, and a macro F1-score of 0.9979, thus asserting its power in the correct identification of normal and attack traffic. On the other hand, the Isolation Forest, which is a total novice in the supervision game, had a mere 0.7631 accuracy and 0.2027 ROC-AUC score; thus, it failed to distinguish between benign and malignant traffics at all. The Isolation Forest has a weak sole performance, but it still contributes important anomaly scores to the ensemble by spotting the kinds of behaviors that the LightGBM predictions overlook through outlier detection.

The Stacked Hybrid model, which combines the outputs of the three methods by a fusion meta-learning layer through autoencoder, LightGBM, and Isolation Forest, got the highest generalization, with an accuracy of 0.9985, a ROC-AUC of 0.9998, and a PR-AUC of 0.9999. The stable precision, recall, and F1-macro metrics for both LightGBM and the hybrid ensemble demonstrate the cooperation between the supervised and unsupervised parts. Thus, the experiments prove that the combination of self-supervised latent embeddings and ensemble decision fusion has a tremendous impact on the detection of both known and zero-day threats while ensuring very high precision and recall.

Table 1. Performance comparison of individual and hybrid models on the TON_IoT dataset.

Model	Accuracy	ROC-AUC	PR-AUC	Threshold	Precision (macro)	Recall (macro)	F1 (macro)
LightGBM	0.9985	1	1	0.27	0.9985	0.9974	0.9979
IsolationForest	0.7631	0.2027	0.6242	0	0.3815	0.5	0.4328
Stacked Hybrid	0.9985	0.9998	0.9999	0.5	0.9984	0.9975	0.9979

The SHAP values of the LightGBM component of HADES-IoT are plotted in Figure 3, which shows the strongest inputs behind the attack decisions. The most significant inputs were all packet-related, starting with Destination Packets and Source Packets, then followed by Flow Duration, Source/Destination IP Bytes, and some latent AE codes like Latent z9, z7, z20, z31. There is a color gradient indicating the magnitude of the raw features: high packet counts (red) usually pull the predictions towards the attack class (positive SHAP), while low counts (blue) most of the time reduce the likelihood of an attack. Byte-volume features have a more or less the same behavior, which indicates that heavy, asymmetric flows are the signature of malicious activity in TON_IoT. Besides, the latent representations which are ranked as one of the most influential features, actually capture non-linear co-variations (like burstiness and directionality) that only partly covered by any single raw counter, thus making the hybrid model superior in distinguishing borderline flows and rare patterns. On the whole, the plot presents the alignment of HADES-IoT's decisions with the intuitive semantics of traffic—packets and byte dynamics being the most important factors—while the AE embeddings are responsible for providing the extra discriminative context that further enhances the model's robustness and aids in zero-day generalization.

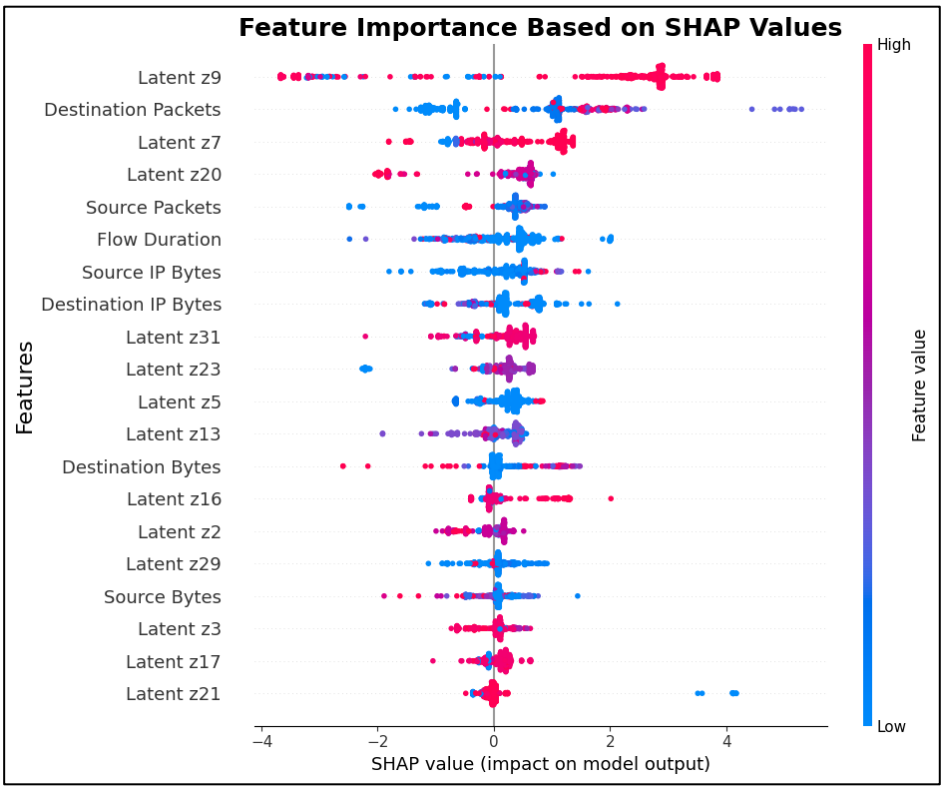

Figure 3. SHAP-based feature importance explaining the contribution of both original and latent features in the LightGBM classifier within the HADES-IoT framework.

4. Discussion

The HADES-IoT hybrid anomaly detection framework presented herein is a major breakthrough in the protection of IoT environments. The advance results from the combination of the self-supervised feature extraction, supervised learning, and unsupervised anomaly detection it makes. The autoencoder latent embeddings are combined with LightGBM and Isolation Forest in the framework making it possible for the model to detect almost all kinds of attacks with close to perfect accuracy using the TON_IoT dataset. The hybrid stacking approach not only improves the system's robustness, however, it also explains better, and its capability to see novel attack types surpasses that of the existing systems which are solely based on either supervised or unsupervised learning.

In the context of previous research, the framework proposed here fits with and broadens the recent advancements in intelligent intrusion detection systems. For example, Krishnaveni et al. [15] presented SmartHive-IDS which made use of SHAP-based feature selection and Bi-LSTM models for protecting ICPS, obtaining an accuracy of 98.96% but with the downside of high computational complexity. On the other hand, Chelghoum et al. [16] employed blockchain along with reinforcement learning to secure 6G-enabled vehicle networks, yet their solution was designed for certain vehicular environments only. Similarly, Qureshi et al. [17] and Benmalek et al. [18] investigated adaptive AI-driven and stacked neural network methods, respectively, in IoT and IoMT applications, providing excellent performance but lacking in interpretability. Nazir et al. [19] used ensemble learning for N-BaIoT-based IoT botnet detection and attained very high accuracy but limited scalability across a wide variety of IoT contexts. Hirsi et al. [20] examined SDN-based DDoS detection using ensemble models; Reddy et al. [21] and Rustam et al. [22] pointed out the potential of deep learning and AI for network security but did not clarify feature-level decisions. Hossain et al. [23] tackled the subject of interpretability with Extra Trees and LIME, demonstrating that transparent AI is crucial for dependable IoT protection.

Our framework not only complements but also advances this area by offering explainability and generalization at the same time. The SHAP-based feature analysis (Figure 3) pointed out that classical traffic metrics like destination packets, flow duration, and byte transfer still hold the strongest sway, while autoencoder-derived latent variables play a significant role in the detection of intricate, delicate anomalies. This interpretative understanding is of utmost importance for the real-world application in industrial and healthcare IoT, where trustable model evaluations are needed by human operators.

From a performance standpoint, the hybrid ensemble performs at least as well as the previous models or even better depending on the metric. The comparison given in Table 1 indicates that LightGBM and the Stacked Hybrid are very close to unity ROC-AUC and PR-AUC values, and they even surpass some deep or reinforcement learning-based models cited in the literature, but they do so whilst consuming less computational power which makes them suitable for real-time IoT gateways.

The HADES-IoT framework proposed for anomaly detection in IoT networks has demonstrated outstanding performance but it can still be extended in several promising ways to make it even more applicable and resilient in real-life scenarios. One of the main opportunities for improvement is to create online and federated learning mechanisms, which would empower the system to be always up to date with the new network patterns without compromising the privacy of the distributed IoT node data. This is an important necessity in the central data-free environment where non-stationary traffic behaviors and new types of attacks have to be handled. Lightweight optimization for edge deployment is another direction for the future, where techniques like model pruning, quantization, and knowledge distillation can be used to cut down computational complexity, thus making the system fit for real-time inference on even the least capable IoT devices.

5. Conclusion

The HADES-IoT anomaly detection framework, which is hybrid, was presented by this research as the solution to the IoT network security problem by using self-supervised feature learning, supervised classification, and unsupervised anomaly detection. The model combines the latent features from the autoencoder with LightGBM and Isolation Forest in a stacked ensemble so that it can easily recognize complicated data patterns, eliminate overfitting, and increase the model's ability to generalize to new types of attacks. The evaluation carried out on the TON_IoT dataset revealed that the performance of the HADES-IoT model is almost flawless since it had a total accuracy of 99.85%, and its ROC-AUC and PR-AUC values are close to 1.0000, thereby, it was the one that had the biggest performance among all other models, including the standalone ones.

The application of SHAP-based interpretability analysis was able to not only confirm the support given by traffic features like packet counts, byte transfers, and flow duration but was also able to provide communication insights in regard to the decision-making process that made such predictions as being valid or not. While the latent autoencoder features capture hidden non-linear relationships that are critical for the detection of subtle and zero-day anomalies. The novel system, in comparison to recent state-of-the-art approaches, merges the explainability of tree-based models with the adaptability of deep learning adopting the trade-off between accuracy, transparency, and computational efficiency.

REFERENCES

[1] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The Internet of Things (IoT) in healthcare: Taking stock and moving forward," *Internet of Things*, vol. 22, p. 100721, 2023.

[2] S. Afrin, S. J. Rafa, M. Kabir, T. Farah, M. S. B. Alam, A. Lameesa, *et al.*, "Industrial Internet of Things: Implementations, challenges, and potential solutions across various industries," *Computers in Industry*, vol. 170, p. 104317, 2025.

[3] B. Rathi, S. Thapaswi, M. Kambhampati, V. Jain, P. Akshay, T. N. Pandey, and S. K. Pradhan, "Realizing the potential of Internet of Things (IoT) in industrial applications," *Discover Internet of Things*, vol. 5, no. 1, pp. 1–16, 2025.

[4] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal, "A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges," *Journal of Information and Intelligence*, vol. 2, no. 6, pp. 455–513, 2024.

[5] A. Nazir, J. He, N. Zhu, A. Wajahat, X. Ma, F. Ullah, *et al.*, "Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets," *Journal of King Saud University–Computer and Information Sciences*, vol. 35, no. 10, p. 101820, 2023.

[6] G. Logeswari, J. D. Roselind, K. Tamilarasi, and V. Nivethitha, "A comprehensive approach to intrusion detection in IoT environments using hybrid feature selection and multi-stage classification techniques," *IEEE Access*, 2025.

[7] L. Shan, "IoT network intrusion detection system using optimization algorithms," *Scientific Reports*, vol. 15, no. 1, p. 21706, 2025.

[8] B. Isong, O. Kgote, and A. Abu-Mahfouz, "Insights into modern intrusion detection strategies for internet of things ecosystems," *Electronics*, vol. 13, no. 12, p. 2370, 2024.

[9] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The significance of machine learning and deep learning techniques in cybersecurity: A comprehensive review," *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, p. 10, 2023.

[10] R. Chinnasamy, M. Subramanian, S. V. Easwaramoorthy, and J. Cho, "Deep learning-driven methods for network-based intrusion detection systems: A systematic review," *ICT Express*, 2025.

[11] M. Zahid and T. S. Bharati, "Enhancing cybersecurity in IoT systems: A hybrid deep learning approach for real-time attack detection," *Discover Internet of Things*, vol. 5, no. 1, p. 73, 2025.

[12] M. Haidarh, C. Mu, Y. Liu, and X. He, "Exploring traditional, deep learning and hybrid methods for hyperspectral image classification: A review," *Journal of Information and Intelligence*, 2025.

[13] K. Berahmand, F. Daneshfar, E. S. Salehi, Y. Li, and Y. Xu, "Autoencoders and their applications in machine learning: A survey," *Artificial Intelligence Review*, vol. 57, no. 2, p. 28, 2024.

[14] H. Bangui, M. Ge, and B. Buhnova, "A hybrid machine learning model for intrusion detection in VANET," *Computing*, vol. 104, no. 3, pp. 503–531, 2022.

[15] S. Krishnaveni, S. Zeadally, S. Sivamohan, and S. S. Sridhar, "SmartHive-IDS: An advanced intrusion detection framework for SDN-HoneyNet enabled ICPS using hybrid explainable ensemble feature selection with optimized Bi-LSTM," *Cluster Computing*, vol. 28, no. 14, p. 913, 2025.

[16] M. Chelghoum, G. Bendiab, M. Benmohammed, S. Bousalem, and A. Mellouk, "Securing 6G-enabled vehicle-to-everything communications: A blockchain-enabled collaborative intrusion detection framework with reinforcement learning," *Computer Networks*, vol. 270, p. 111568, 2025.

[17] S. S. Qureshi, J. He, N. Zhu, S. Dhelim, and M. S. Pathan, "Enhancing IoT security and healthcare data protection in the metaverse: A dynamic adaptive security mechanism," *Egyptian Informatics Journal*, vol. 30, p. 100670, 2025.

[18] M. Benmalek, A. Seddiki, and K.-D. Haouam, "SNN-IoMT: A novel AI-driven model for intrusion detection in Internet of Medical Things," *CMES–Computer Modeling in Engineering and Sciences*, vol. 143, no. 1, pp. 1157–1184, 2025.

[19] A. Nazir, J. He, N. Zhu, S. U. Qureshi, and A. Wajahat, "Ensemble learning techniques for the detection of IoT botnets," in *Proc. ACM Int. Conf.*, 2024, pp. 80–85.

[20] A. Hirsi, L. Audah, A. Salh, M. A. Alhartomi, and S. Ahmed, "Detecting low-rate DDoS attacks in SDN using ensemble machine learning techniques," in *Proc. IEEE SCOReD*, 2024, pp. 299–304.

[21] V. Reddy, R. Sunitha, M. Anusha, S. Chaitra, and A. P. Kumar, "Artificial intelligence based intrusion detection systems," in *Proc. IEEE ICMNWC*, 2024.

[22] F. Rustam, P. Ranaweera, and A. D. Jurcut, "AI on the defensive and offensive: Securing multi-environment networks from AI agents," in *Proc. IEEE ICC*, 2024, pp. 4287–4292.

[23] M. A. Hossain, S. Saif, and M. S. Islam, "Interpretable machine learning for IoT security," in *Proc. ICIESTR*, 2024.

[24] M. F. Hasan, M. H. Moon, and D. M. Raza, "IoT network intrusion detection using ensemble learning approach," in *Proc. ICCCNT*, 2023.