

Similarity-driven intrusion detection for cloud-centric internet of things networks

Jawahar Muthusamy¹, Palani Latha², Rajakumar Ponnumani³, Anubhav Kumar⁴, Rajakumar Perumal⁵, Prabu Kaliyaperumal⁶

¹School of Computer Science and Engineering, VIT-AP University, Andhra Pradesh, India

²Department of Information Technology, Panimalar Engineering College, Chennai, India

³Department of Computer Science and Engineering, Parul Institute of Technology, Faculty of Engineering and Technology, Parul University, Vadodara, India

⁴Department of Computer Science and Engineering, Faculty of Engineering and Technology, HRIT University, Ghaziabad, India

⁵Department of Computer Science and Applications, Sharda School of Computing Science and Engineering, Sharda University, Greater Noida, India

⁶School of Computer Science and Engineering, IILM University, Greater Noida, India

Article Info

Article history:

Received Jul 4, 2026

Revised Aug 22, 2026

Accepted Sep 4, 2026

Keywords:

Cloud-centric internet of thing
Explainable artificial intelligent
Intrusion detection
SHapley Additive exPlanation
Siamese Bi-LSTM
Similarity learning

ABSTRACT

Cloud-centric internet of things (IoT) environments continuously generates heterogeneous network traffic, making intrusion detection increasingly challenging as attack behaviors evolve beyond previously observed patterns. Conventional intrusion detection systems (IDS) rely primarily on supervised classification, limiting their ability to generalize to unseen threats while providing limited explanation for detection decisions. This paper proposes similarity-driven intrusion detection framework (SiamIDS), a SiamIDS that employs behavioral similarity learning to identify malicious network traffic. The framework integrates an autoencoder for feature compression with a Siamese bidirectional long short-term memory (Bi-LSTM) network for temporal similarity modeling, while SHapley Additive exPlanations (SHAP) provide feature-level explanations and ordering points to identify the clustering structure (OPTICS) supports post-detection behavioral analysis of anomalous traffic. The proposed framework was evaluated on the CIC IoT-DIAD 2024 dataset and compared with representative baseline deep learning models. Experimental results achieved an overall accuracy of 99.76%, precision of 95.62%, recall of 98.98%, and an F1-score of 97.24%, demonstrating consistent detection performance across seven attack families. Reconstruction loss analysis confirmed stable latent feature learning, while SHAP explanations showed that multiple network attributes collectively influenced intrusion decisions. These findings demonstrate that behavioral similarity learning provides an accurate and interpretable solution for intrusion detection in cloud-centric IoT environments.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Prabu Kaliyaperumal
School of Computer Science and Engineering, IILM University
Greater Noida, Uttar Pradesh, India
Email: mega.prabu@gmail.com

1. INTRODUCTION

The rapid expansion of internet of things (IoT) deployments has transformed the way data are collected, processed, and exchanged across smart homes, industrial automation, healthcare, transportation, and critical infrastructure [1], [2]. As billions of heterogeneous devices continuously communicate through cloud

platforms, the volume and diversity of network traffic have increased substantially, creating new opportunities for intelligent services while simultaneously enlarging the cyberattack surface [3], [4]. The distributed nature of cloud-centric IoT environments, combined with constrained device resources and heterogeneous communication protocols, makes them attractive targets for attacks such as distributed denial-of-service (DDoS), reconnaissance, spoofing, botnets, and web-based intrusions [5], [6]. Consequently, intrusion detection systems (IDS) have become an indispensable security component for identifying malicious activities before they compromise network availability, confidentiality, or integrity [7]. However, maintaining high detection accuracy in dynamic IoT environments remains challenging because attack characteristics continuously evolve, often differing from those observed during model training [8], [9].

Conventional machine learning and deep learning-based IDS generally formulate intrusion detection as a multi-class classification problem, where models learn decision boundaries directly from labeled attack categories [10]. Although these approaches achieve high performance on benchmark datasets, their effectiveness often declines when network behavior deviates from previously observed patterns or when previously unseen attacks emerge [11], [12]. Furthermore, many existing models emphasize predictive performance while providing limited insight into why a traffic flow is classified as malicious, reducing their usefulness for security analysts during incident investigation [13], [14]. These limitations indicate that effective intrusion detection should move beyond attack label memorization and instead learn behavioral relationships that remain relatively stable even when attack implementations evolve.

Recent studies have explored various deep learning architectures to improve intrusion detection performance in IoT networks. Amareshwari and Govardhanis [15] developed a bidirectional long short-term memory (Bi-LSTM)-based intrusion detection model that effectively captured temporal dependencies in network traffic and demonstrated high detection accuracy on benchmark datasets. Mareeswari and Balasubramanian [16] investigated Bi-LSTM deployment within distributed cloud-edge environments, showing that sequence learning can improve scalability while reducing computational overhead. Hnamte and Hussain [17] proposed a hybrid DCNN-Bi-LSTM architecture that combined convolutional feature extraction with temporal learning, achieving excellent classification performance for industrial IoT traffic. More recently, Ahman *et al.* [18] integrated CNN and Bi-LSTM models for software-defined networking environments, demonstrating the benefits of combining spatial and temporal representations. Likewise, Zhang *et al.* [19] incorporated multi-head attention into Bi-LSTM networks to strengthen contextual feature learning and improve classification accuracy across multiple intrusion detection datasets. Although these studies demonstrate the effectiveness of temporal deep learning models, they primarily rely on supervised classification, limiting their ability to adapt to evolving or previously unseen attack behaviors.

To improve generalization, several researchers have investigated similarity learning, explainable artificial intelligence, and advanced anomaly analysis. Hindy *et al.* [20] introduced Siamese learning for zero-day attack detection by measuring similarity between network traffic pairs instead of relying solely on conventional classification. Althiyabi *et al.* [21] employed few-shot learning with prototypical networks to improve detection under limited labeled data, while Bo *et al.* [22] further enhanced prototype learning through adaptive feature fusion. From an interpretability perspective, Alabbadi and Bajaber [23] demonstrated that SHapley Additive exPlanations (SHAP) explanations substantially improve the transparency of deep learning-based IDS, enabling analysts to understand model decisions. Nevertheless, most existing studies improve only individual aspects of intrusion detection. Temporal sequence learning, behavioral similarity modeling, explainable prediction, and post-detection behavioral analysis are generally investigated independently rather than within a unified detection framework. Consequently, security analysts still face challenges in identifying evolving attack behaviors while simultaneously understanding the rationale behind detection decisions.

Motivated by these observations, this paper proposes similarity-driven intrusion detection framework (SiamIDS), a SiamIDS for cloud-centric IoT networks. Instead of directly learning attack categories, SiamIDS models behavioral similarity between network traffic sequences using a Siamese Bi-LSTM architecture. A lightweight autoencoder first compresses high-dimensional traffic features into compact latent representations that preserve essential behavioral characteristics while reducing computational complexity. The learned similarity representations are subsequently interpreted using SHAP to provide feature-level explanations, and detected anomalies are organized through ordering points to identify the clustering structure (OPTICS) clustering to facilitate behavioral analysis. Experimental evaluation on the CIC IoT-DIAD 2024 dataset demonstrates that the proposed framework provides accurate and interpretable intrusion detection while maintaining practical deployment efficiency for large-scale cloud-centric IoT environments.

The major contributions of this work are summarized as follows:

- A SiamIDS is proposed that models behavioral relationships among IoT traffic sequences instead of directly learning attack labels, improving the capability to recognize evolving malicious behaviors.

- A Siamese Bi-LSTM architecture with autoencoder-based feature compression is developed to jointly capture temporal dependencies and behavioral similarity while reducing computational complexity associated with high-dimensional IoT traffic.
- An explainable intrusion analysis mechanism is incorporated by integrating SHAP for feature-level interpretation and OPTICS clustering for grouping detected anomalies into meaningful behavioral patterns.
- Comprehensive experiments on the CIC IoT-DIAD 2024 dataset demonstrate that the proposed framework achieves competitive intrusion detection performance while providing transparent decision support suitable for cloud-centric IoT security applications.

2. METHOD

Figure 1 presents the overall workflow of the proposed SiamIDS framework. Network traffic collected from the cloud-centric IoT environment is first normalized and transformed into fixed-length flow sequences. The normalized traffic is then compressed using a lightweight autoencoder to obtain compact latent representations while preserving the behavioral characteristics of each communication flow. These representations are processed by a Siamese Bi-LSTM network that learns the similarity between traffic sequences instead of directly assigning attack labels. During inference, the similarity between an incoming traffic sequence and benign reference embeddings is used to determine whether the observed behavior deviates from normal network activity. To improve the transparency of the detection process, SHAP is employed to quantify the contribution of individual traffic features to each prediction. Finally, OPTICS groups the detected anomalies into behaviorally similar clusters, assisting post-detection analysis without affecting the classification process.

Unlike conventional supervised IDS, SiamIDS learns relationships between network behaviors rather than relying solely on predefined attack categories. The intuition is that benign traffic generally exhibits stable communication patterns, whereas malicious traffic introduces behavioral deviations even when the attack type has not been encountered during training. Learning this behavioral similarity enables the detector to generalize beyond known attack labels while reducing dependence on highly balanced training datasets.

The first stage of the framework performs feature normalization and dimensionality reduction. Given an input traffic vector x , each feature is standardized using Z-score normalization,

$$x'_i = \frac{x_i - \mu_i}{\sigma_i} \quad (1)$$

where μ_i and σ_i denote the mean and standard deviation of the corresponding feature. Normalization prevents features with large numerical ranges from dominating the optimization process and improves convergence during neural network training.

The normalized traffic is then passed through a shallow autoencoder. Instead of manually selecting features, the encoder learns a compact latent representation that preserves the dominant behavioral characteristics of each traffic flow while reducing feature redundancy. The encoder output is expressed as (2):

$$z = \phi(W_e x + b_e) \quad (2)$$

where W_e and b_e denote the encoder parameters and $\phi()$ represents the activation function. The latent vector z becomes the input to the similarity learning stage. Using compressed representations substantially reduces computational complexity while preserving the temporal information required for intrusion detection.

Behavioral similarity is learned through two identical Bi-LSTM branches with shared parameters. The 20-dimensional latent representation generated by the autoencoder is provided to both branches. Each branch uses 64 hidden units in each direction, and the forward and backward states are concatenated to form a 128-dimensional temporal embedding. The shared weights ensure that both branches map the input sequences into the same representation space, enabling direct comparison of their behavioral patterns. The sequence representation generated by the Bi-LSTM is defined as (3):

$$h_t = \overrightarrow{h}_t | \overleftarrow{h}_t \quad (3)$$

where $\overrightarrow{h}_t$ and $\overleftarrow{h}_t$ represent the forward and backward hidden states, respectively, and $|$ denotes vector concatenation. The resulting embedding captures both past and future temporal dependencies within the network flow, providing richer behavioral information than a unidirectional sequence model.

The embeddings produced by the two branches are compared using contrastive learning. Positive pairs consist of two benign traffic sequences, whereas negative pairs contain one benign and one malicious sequence. The Siamese model was trained with 200,000 pairs, equally divided into 100,000 positive and 100,000 negative

pairs. An independently generated set of 20,000 validation pairs with equal positive and negative composition was used for similarity-threshold selection. A separate set of 10,000 benign sequences was retained as the reference set for inference, while the test sequences were kept isolated until final evaluation. During optimization, the network minimizes the distance between positive pairs while increasing the distance between negative pairs. The Euclidean distance between the two latent embeddings is computed as $d = |z_1 - z_2|_2$. The contrastive objective is expressed as (4):

$$L = (1 - y) \frac{1}{2} d^2 + y \frac{1}{2} \max(0, m - d)^2 \quad (4)$$

where d denotes the Euclidean distance, y indicates whether the pair is similar or dissimilar, and m is the separation margin, set to 1.0 in the experiments. The loss pulls similar pairs closer in the embedding space and separates dissimilar pairs when their distance falls below the specified margin. Rather than predicting attack classes directly, the learned embedding space enables the framework to identify abnormal behavior through similarity measurements, making the model more tolerant of evolving attack patterns.

Once an intrusion has been identified, SiamIDS provides an explanation of the prediction using SHAP. Instead of treating the neural network as a black box, SHAP estimates the contribution of each traffic feature to the final prediction, allowing analysts to understand which network characteristics influenced the anomaly decision. The additive explanation model is expressed as (5):

$$f(x) = \phi_0 + \sum_{i=1}^n \phi_i \quad (5)$$

where ϕ_i represents the contribution of the i^{th} feature and ϕ_0 denotes the expected model output. These explanations are generated only after the detection stage and therefore do not increase inference complexity.

Finally, the latent representations corresponding to anomalous traffic are analyzed using OPTICS clustering. Instead of creating a fixed number of clusters, OPTICS groups traffic according to density, enabling similar attack behaviors to be organized together while isolating outliers. This post-processing stage assists security analysts in identifying related attack campaigns and facilitates behavioral investigation without influencing the primary intrusion decision.

SiamIDS follows a sequential workflow in which feature compression, temporal similarity learning, explainable prediction, and behavioral clustering complement one another. The autoencoder reduces input complexity, the Siamese Bi-LSTM performs similarity-driven intrusion detection, SHAP explains individual predictions, and OPTICS organizes detected anomalies into meaningful behavioral groups. By separating detection from interpretation and post-analysis, the framework maintains a compact architecture while providing both accurate intrusion identification and practical decision support for cloud-centric IoT environments.

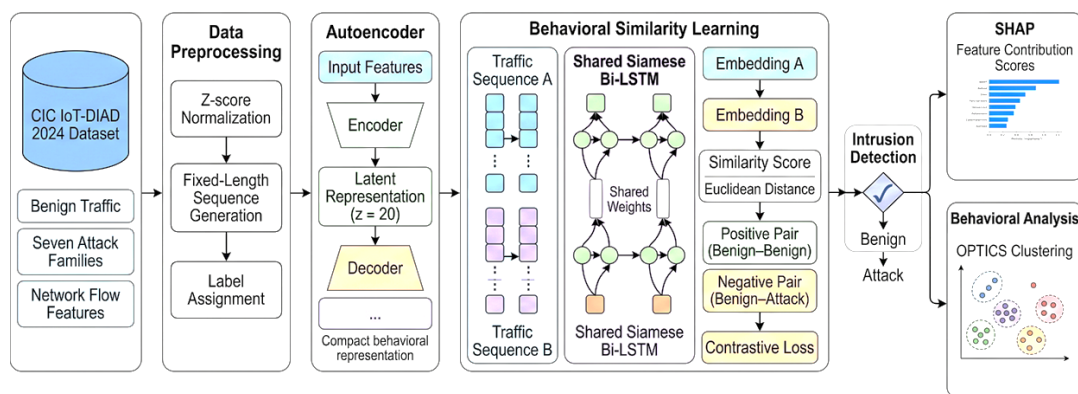


Figure 1. Overall workflow of the proposed SiamIDS framework integrating feature compression, behavioral similarity learning, intrusion detection, explainability, and behavioral analysis

3. RESULTS AND DISCUSSION

3.1. Experimental configuration

The proposed SiamIDS framework was evaluated using the CIC IoT-DIAD 2024 [24] dataset containing benign traffic and seven major attack families. All baseline models were trained and evaluated using

the same preprocessing pipeline, 70:10:20 train-validation-test split, and hyperparameter optimization procedure to ensure a fair comparison. Performance was assessed using precision, recall, F1-score, and overall accuracy. For multiclass evaluation, the reported overall precision, recall, and F1-score correspond to macro-averaged values across all attack families, whereas overall accuracy represents the proportion of correctly classified samples over the complete test set. In addition to classification performance, the evaluation considered representation quality through reconstruction loss and model interpretability using SHAP feature attribution. Each experiment was repeated five times, and the reported results represent the mean performance across all runs. The main hyperparameter settings used for the autoencoder and Siamese Bi-LSTM stages are summarized in Table 1.

Table 1. Hyperparameter configuration of the proposed SiamIDS framework

Component	Parameter	Value	Component	Parameter	Value
Autoencoder	Latent dimension	20	Siamese Bi-LSTM	Optimizer	Adam
Autoencoder	Optimizer	Adam	Siamese Bi-LSTM	Learning rate	0.001
Autoencoder	Learning rate	0.001	Siamese Bi-LSTM	Batch size	256
Autoencoder	Batch size	512	Siamese Bi-LSTM	Epochs	30
Autoencoder	Epochs	39	Siamese Bi-LSTM	Contrastive margin	1.0
Siamese Bi-LSTM	Hidden units/direction	64	Siamese Bi-LSTM	Distance metric	Euclidean
Siamese Bi-LSTM	Embedding dimension	128	Siamese Bi-LSTM	Dropout	0.30

The hyperparameters were selected after preliminary experiments to balance detection performance and model stability. A latent dimension of 20 provided compact feature representations while preserving the essential behavioral characteristics of network traffic. The Siamese Bi-LSTM architecture with shared weights effectively captured temporal dependencies and behavioral similarity among traffic sequences. The Adam optimizer enabled stable convergence throughout training without requiring extensive hyperparameter adjustment.

3.2. Performance evaluation

The training behavior of the autoencoder was examined using reconstruction MSE, as shown in Figure 2. Both validation and testing curves exhibit a progressive reduction in error, reaching values below 0.02 toward the later epochs. Their close agreement indicates stable reconstruction behavior without noticeable overfitting. The result suggests that the 20-dimensional latent representation preserves relevant traffic characteristics while reducing feature redundancy, providing compact inputs for the subsequent Siamese Bi-LSTM. The final Siamese configuration was selected through validation-based tuning of the learning parameters and contrastive margin and was then used for the reported evaluation.

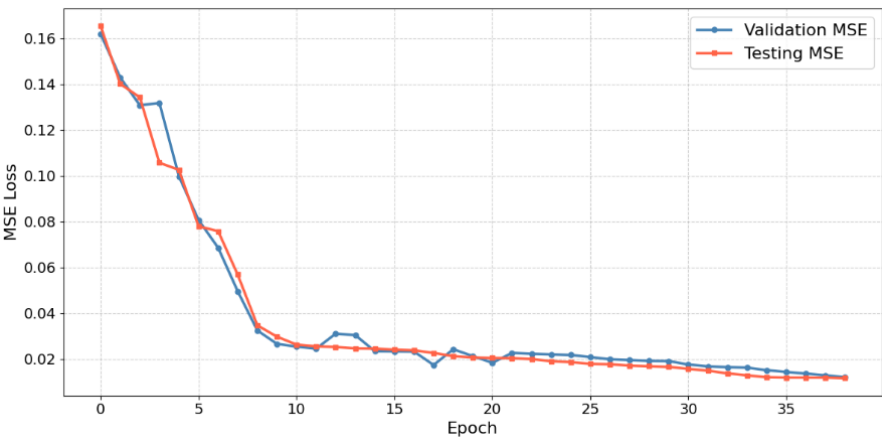


Figure 2. Validation and testing mean squared error (MSE) during autoencoder training for latent feature representation learning

Table 2 summarizes the multiclass detection performance of SiamIDS across seven attack families. The proposed framework consistently achieves high detection performance, with DDoS and DoS attacks recording F1-scores above 98.9%, demonstrating that the Siamese Bi-LSTM effectively captures the temporal

characteristics of high-volume network attacks. Reconnaissance and spoofing attacks also exhibit strong precision and recall, indicating that behavioral similarity learning remains reliable across diverse traffic patterns. Compared with the remaining attack categories, Mirai and web-based attacks show relatively lower precision, which can be attributed to the limited number of representative samples and the overlap of their communication behavior with other attack classes. Nevertheless, both categories maintain recall values close to 99%, indicating that the framework successfully identifies the majority of malicious traffic while minimizing false negatives. SiamIDS achieved an accuracy of 99.76%, precision of 95.62%, recall of 98.98%, and an F1-score of 97.24%, demonstrating stable intrusion detection performance across heterogeneous IoT attack categories.

Table 2. Intrusion detection performance of SiamIDS across different attack families

Attack family	Precision	Recall	F1-score	Accuracy
BruteForce	0.9891	0.9890	0.9889	0.9999
DDoS	0.9883	0.9914	0.9898	0.9942
DoS	0.9982	0.9919	0.9951	0.9936
Mirai	0.9081	0.9899	0.9472	0.9984
Recon	0.9543	0.9888	0.9712	0.9979
Spoofing	0.9551	0.9901	0.9723	0.9993
Web-based	0.9006	0.9881	0.9423	0.9999
Overall	0.9562	0.9898	0.9724	0.9976

The multiclass confusion matrix presented in Figure 3 provides further insight into the classification behavior. Most attack families form dominant diagonal patterns, indicating correct classification of the majority of traffic flows. The largest confusion occurs between DoS and DDoS attacks because both generate high-volume flooding traffic with similar temporal communication characteristics. A smaller degree of overlap is observed between reconnaissance and spoofing traffic, reflecting similarities in network probing behavior. Despite these overlaps, the number of misclassified samples remains relatively small compared with the overall dataset, suggesting that the learned behavioral similarity space effectively separates different attack categories. The consistently high recall across all attack families further indicates that SiamIDS captures common malicious communication patterns without relying solely on rigid attack-specific decision boundaries.

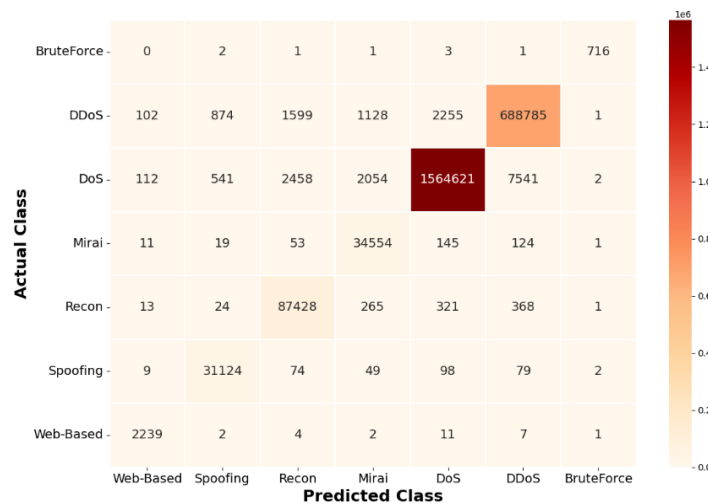


Figure 3. Confusion matrix of SiamIDS for multiclass intrusion detection across seven attack families

Table 3 compares SiamIDS with representative baseline deep learning models evaluated under an identical experimental configuration using the same train-validation-test split and preprocessing pipeline. CNN and LSTM establish conventional spatial and temporal learning baselines, while Bi-LSTM demonstrates the benefit of bidirectional sequence modeling for network traffic analysis. Incorporating the Siamese architecture further improves behavioral discrimination by learning relationships between traffic sequences instead of relying solely on attack labels. The proposed SiamIDS framework achieved the highest overall performance, attaining an accuracy of 99.76%, precision of 95.62%, recall of 98.98%, and an F1-score of 97.27%.

Table 3. Comparative evaluation of SiamIDS against baseline deep learning models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)	Training time (min)	Inference time (ms/sample)
CNN [25]	96.97	92.81	95.23	94.01	24.5	1.32
LSTM [26]	98.11	93.87	96.14	94.99	30.7	2.05
Bi-LSTM [27]	98.97	95.01	97.22	96.1	36.8	2.64
Siamese Bi-LSTM [28]	99.01	95.13	98.02	96.55	40.3	3.11
SiamIDS	99.76	95.62	98.98	97.27	34.9	2.58

Compared with the Siamese Bi-LSTM baseline, the improvement is achieved through autoencoder-based latent feature representation, which provides compact inputs for behavioral similarity learning without increasing computational cost. This is reflected by the reduction in training time from 40.3 min to 34.9 min and inference time from 3.11 ms/sample to 2.58 ms/sample. While SHAP and OPTICS do not directly improve classification accuracy, they enhance the interpretability of detection decisions and facilitate behavioral analysis of anomalous traffic. The progressive improvement from CNN to SiamIDS demonstrates that behavioral similarity learning effectively complements temporal sequence modeling while maintaining practical computational efficiency. Interpretability is illustrated in Figure 4, which presents the three most influential SHAP features for six representative anomalous traffic sequences.

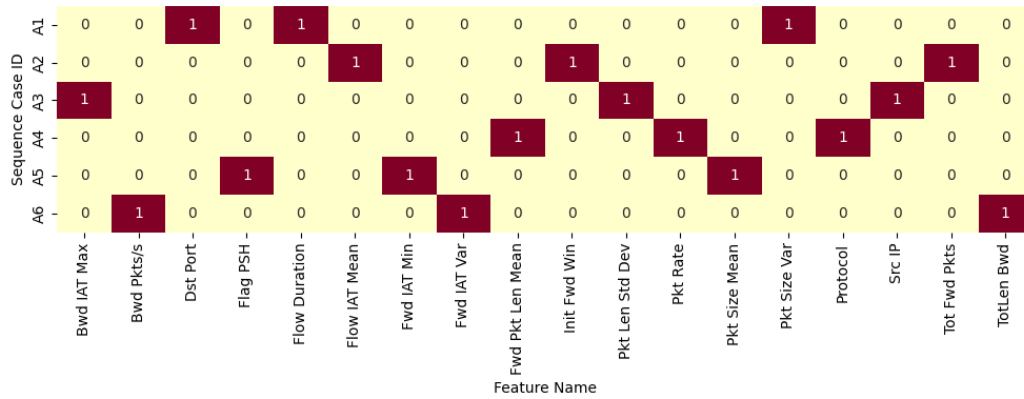


Figure 4. SHAP-based feature attribution for representative anomalous cases

Although the dominant features vary across individual cases, attributes related to packet length, flow duration, inter-arrival time, packet rate, protocol information, and forward or backward packet statistics consistently contribute to the final predictions. This variation indicates that SiamIDS does not rely on a single discriminative feature; instead, it learns behavioural relationships from multiple complementary traffic characteristics. The SHAP explanations therefore provide meaningful evidence supporting each anomaly decision, allowing security analysts to understand why a particular traffic flow is considered suspicious rather than treating the detector as a black-box model.

4. DISCUSSION

The experimental results indicate that behavioral similarity learning provides an effective approach to conventional label-based intrusion detection. Instead of relying exclusively on predefined attack categories, SiamIDS compares traffic sequences in a shared embedding space, enabling the model to distinguish malicious behaviors that exhibit temporal patterns different from benign communication. The consistently high recall across all attack families suggests that the proposed similarity-learning strategy effectively captures common malicious communication patterns, including attack categories with comparatively fewer representative samples. The baseline comparison further demonstrates that combining autoencoder-based feature compression with Siamese Bi-LSTM learning consistently improves detection performance over conventional deep learning architectures while maintaining practical training and inference efficiency. Furthermore, the SHAP analysis shows that the detection decisions are influenced by multiple complementary traffic attributes rather than a single dominant feature, improving the interpretability of the detection process during security analysis. Although the framework achieved strong performance on the CIC IoT-DIAD 2024 dataset, its evaluation is currently limited to a single benchmark dataset. Future work will investigate cross-dataset

validation and adaptive behavioral similarity learning under continuously evolving network traffic to further assess the robustness and generalization capability of the proposed framework.

5. CONCLUSION

This paper presented SiamIDS, a SiamIDS developed for cloud-centric IoT networks. Unlike conventional supervised IDSs that directly learn attack labels, SiamIDS models behavioral similarity between network traffic sequences using a Siamese Bi-LSTM architecture. An autoencoder compresses high-dimensional traffic into compact latent representations, while SHAP provides feature-level explanations of detection decisions and OPTICS facilitates post-detection behavioral analysis of anomalous traffic. Experimental evaluation on the CIC IoT-DIAD 2024 dataset, including comparisons with representative baseline deep learning models, demonstrated consistent detection performance across seven attack families, achieving an overall accuracy of 99.76%, precision of 95.62%, recall of 98.98%, and an F1-score of 97.24%. These results indicate that learning behavioral similarity enables accurate and interpretable intrusion detection while reducing reliance on rigid attack-specific decision boundaries. The proposed framework therefore provides a practical solution for cloud-centric IoT environments that require both reliable detection and transparent decision support. Future work will investigate cross-dataset validation, adaptive similarity learning for evolving attack behaviors, and lightweight deployment strategies for resource-constrained edge devices to further improve the generalization capability of SiamIDS.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Jawahar Muthusamy	✓			✓		✓		✓		✓			✓	
Palani Latha		✓			✓			✓	✓		✓	✓		✓
Rajakumar Ponnumani	✓		✓			✓	✓			✓				
Anubhav Kumar		✓		✓		✓		✓	✓			✓		
Rajakumar Perumal	✓		✓		✓			✓		✓		✓		
Prabu Kaliyaperumal	✓	✓		✓		✓	✓		✓	✓	✓			

C : C onceptualization	I : I nterpretation	Vi : V isualization
M : M ethodology	R : R esources	Su : S upervision
So : S oftware	D : D ata Curation	P : P roject administration
Va : V alidation	O : Writing - O riginal Draft	Fu : F unding acquisition
Fo : F ormal analysis	E : Writing - Review & E ditng	

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author, [initials: P.K], upon reasonable request.

REFERENCES

[1] A. Komal and S. Li, "Intrusion Detection in the Internet of Things: A Comprehensive Review of Techniques, Architectures, Datasets, and Emerging Trends," *Sensors*, vol. 26, no. 11, p. 3405, May 2026, doi: 10.3390/s26113405.

[2] M. Luo *et al.*, "HloT: heterogeneous information network based compromised IoT device detection," *Cybersecurity*, vol. 9, no. 1, p. 55, Apr. 2026, doi: 10.1186/s42400-025-00465-3.

[3] F. C. Andriulo, M. Fiore, M. Mongiello, E. Traversa, and V. Zizzo, "Edge Computing and Cloud Computing for Internet of Things: A Review," *Informatics*, vol. 11, no. 4, p. 71, Sep. 2024, doi: 10.3390/informatics11040071.

- [4] I. Ortega-Fernandez, M. Sestelo, J. C. Burguillo, and C. Piñón-Blanco, "Network intrusion detection system for DDoS attacks in ICS using deep autoencoders," *Wireless Networks*, vol. 30, no. 6, pp. 5059–5075, Aug. 2024, doi: 10.1007/s11276-022-03214-3.
- [5] Y. Xiao, Y. Feng, and K. Sakurai, "An Efficient Detection Mechanism of Network Intrusions in IoT Environments Using Autoencoder and Data Partitioning," *Computers*, vol. 13, no. 10, Oct. 2024, doi: 10.3390/computers13100269.
- [6] Y. Li, Z. Li, and M. Li, "A comprehensive survey on intrusion detection algorithms," *Computers and Electrical Engineering*, vol. 121, Jan. 2025, doi: 10.1016/j.compeleceng.2024.109863.
- [7] M. Al Amin, M. S. Ahsan, R. Islam, M. Ahmed, M. F. Mridha, and M. J. Hossen, "Dual-Encoder Adversarial Learning for Cloud-Based Cyber Intrusion Detection," *IEEE Open Journal of the Computer Society*, 2025, doi: 10.1109/OJCS.2025.3637858.
- [8] S. Chen and X. Fang, "Enhancing security in IoT-fog environments with a hybrid deep learning intrusion detection system," *Cluster Computing*, vol. 28, no. 15, p. 1001, 2025, doi: 10.1007/s10586-025-05714-1.
- [9] S. Sadhwani, A. Navare, A. Mohan, R. Muthalagu, and P. M. Pawar, "IoT-based intrusion detection system using explainable multi-class deep learning approaches," *Computers and Electrical Engineering*, vol. 123, Apr. 2025, doi: 10.1016/j.compeleceng.2025.110256.
- [10] A. B. Boudaine, D. Moussaoui, M. Hadjila, W. Ferhi, and M. H. Hachemi, "Deep Learning-Based Anomaly and Intrusion Detection Using the CSE-CIC-IDS2018 Dataset," *Engineering, Technology and Applied Science Research*, vol. 15, no. 4, pp. 24782–24787, Aug. 2025, doi: 10.48084/etasr.11173.
- [11] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly Detection IDS for Detecting DoS Attacks in IoT Networks Based on Machine Learning Algorithms," *Sensors*, vol. 24, no. 2, Jan. 2024, doi: 10.3390/s24020713.
- [12] I. Ficili, M. Giacobbe, G. Tricomi, and A. Puliafito, "From Sensors to Data Intelligence: Leveraging IoT, Cloud, and Edge Computing with AI," *Sensors*, vol. 25, no. 6, p. 1763, Mar. 2025, doi: 10.3390/s25061763.
- [13] B. Nugraha, A. V. Jnanashree, and T. Bauschert, "A versatile XAI-based framework for efficient and explainable intrusion detection systems," *Annals of Telecommunications*, vol. 80, no. 11–12, pp. 1095–1120, Dec. 2025, doi: 10.1007/s12243-025-01118-9.
- [14] F. S. Alsubaei, "Luminous adaptive defense: XAI-driven adaptive security for critical IoT infrastructures," *Journal of Cloud Computing*, vol. 15, no. 1, p. 16, Jan. 2026, doi: 10.1186/s13677-025-00834-w.
- [15] N. R. Amareshwari and A. Govardhanis, "An adaptive cheetah optimization-driven Bi-LSTM framework for efficient network intrusion detection," *International Journal of Data Science and Analytics*, vol. 22, no. 1, p. 173, Dec. 2026, doi: 10.1007/s41060-026-01122-9.
- [16] G. Mareeswari and C. Balasubramanian, "An Intelligent Task Offloading and Data Caching Framework for Mobile Edge Computing Using Bi-LSTM and ODQN," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, Mar. 2026, doi: 10.1007/s40998-026-01048-9.
- [17] V. Hnamte and J. Hussain, "DCNNBiLSTM: An Efficient Hybrid Deep Learning-Based Intrusion Detection System," *Telematics and Informatics Reports*, vol. 10, Jun. 2023, doi: 10.1016/j.teler.2023.100053.
- [18] M. Y. Ahman, S. E.-Y. Abdullahi, and S. A. Adetunji, "A Hybrid CNN–BiLSTM Framework with LightGBM Stacking, SDN-Gate, and PSO-Based Threshold Optimization for Enhanced Intrusion Detection in SDN Environments," *Engineering, Technology & Applied Science Research*, vol. 16, no. 3, pp. 36401–36407, Jun. 2026, doi: 10.48084/etasr.18497.
- [19] J. Zhang, X. Zhang, Z. Liu, F. Fu, Y. Jiao, and F. Xu, "A Network Intrusion Detection Model Based on BiLSTM with Multi-Head Attention Mechanism," *Electronics (Switzerland)*, vol. 12, no. 19, Oct. 2023, doi: 10.3390/electronics12194170.
- [20] H. Hindy *et al.*, "Leveraging siamese networks for one-shot intrusion detection model," *Journal of Intelligent Information Systems*, vol. 60, no. 2, pp. 407–436, Apr. 2023, doi: 10.1007/s10844-022-00747-z.
- [21] T. Althiyabi, I. Ahmad, and M. O. Alassafi, "Enhancing IoT Security: A Few-Shot Learning Approach for Intrusion Detection," *Mathematics*, vol. 12, no. 7, Apr. 2024, doi: 10.3390/math12071055.
- [22] J. Bo, K. Chen, S. Li, and P. Gao, "Boosting Few-Shot Network Intrusion Detection with Adaptive Feature Fusion Mechanism," *Electronics (Switzerland)*, vol. 13, no. 22, Nov. 2024, doi: 10.3390/electronics13224560.
- [23] A. Alabbadi and F. Bajaber, "An Intrusion Detection System over the IoT Data Streams Using eXplainable Artificial Intelligence (XAI)," *Sensors*, vol. 25, no. 3, Feb. 2025, doi: 10.3390/s25030847.
- [24] M. Rabbani *et al.*, "Device Identification and Anomaly Detection in IoT Environments," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 13625–13643, 2025, doi: 10.1109/JIOT.2024.3522863.
- [25] A. Kaissar, A. B. Nassif, B. Soudan, and M. Injadat, "Enhancing CNN-based network intrusion detection through hyperparameter optimization," *Intelligent Systems with Applications*, vol. 26, p. 200528, Jun. 2025, doi: 10.1016/j.iswa.2025.200528.
- [26] N. Dash, S. Chakravarty, A. K. Rath, N. C. Giri, K. M. AboRas, and N. Gowtham, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," *Scientific Reports*, vol. 15, no. 1, p. 1554, Jan. 2025, doi: 10.1038/s41598-025-85248-z.
- [27] S. S. N. Chintapalli, S. P. Singh, J. Frnda, P. B. Divakarachari, V. L. Sarraju, and P. Falkowski-Gilski, "OOA-modified Bi-LSTM network: An effective intrusion detection framework for IoT systems," *Heliyon*, vol. 10, no. 8, Apr. 2024, doi: 10.1016/j.heliyon.2024.e29410.
- [28] H. Cheng, "Cybersecurity classification using Siam-BLA and small-sample data," *Discover Applied Sciences*, Jun. 2026, doi: 10.1007/s42452-026-09047-5.

BIOGRAPHIES OF AUTHORS



Dr. Jawahar Muthusamy     is an Associate Professor in the School of Computer Science and Engineering at VIT-AP University, Andhra Pradesh. Holding a Ph.D., alongside Bachelor's and Master's degrees from Anna University, he brings over 17 years of academic and administrative experience. His robust research portfolio features 35 publications, three textbooks, and six patents. He has core research interests encompass algorithms, cryptography, network security, and cloud computing. He can be contacted at email: jawahar.muthusamy@vitap.ac.in.



Dr. Palani Latha    is a Professor in Department of Information Technology at Panimalar Engineering College, accumulating 25 years of teaching experience. She earned her Ph.D. record with 8 patents, and 22 research papers published in esteemed international journals and conferences. Her expertise spans wireless ad-hoc networks, IoT, and artificial intelligence. She can be contacted at email: latha8201@gmail.com.



Mr. Rajakumar Ponnunani    is an Assistant Professor in the Department of Computer Science and Engineering at Parul Institute of Technology, Parul University, Vadodara, Gujarat, India, with 17 years of teaching experience. He is pursuing a Ph.D. at Galgotias University and has published over 25 international journal and conference papers. His research interests include artificial intelligence, cybersecurity, and cloud computing. He can be contacted at email: prajakumarkk@gmail.com.



Dr. Anubhav Kumar    is a Professor and Dean of Academic Affairs in the Faculty of Engineering and Technology, HRIT University Ghaziabad. Holding a Ph.D. and bringing 24 years of teaching experience, his core expertise spans machine learning, deep learning, data science, NLP, networks, and big data. He has a strong research portfolio featuring 15 patents, 12 book chapters, and 29 research papers published in esteemed international journals and conferences. He can be contacted at email: dr.anubhavkumar@gmail.com.



Mr. Rajakumar Perumal    is an Assistant Professor in Department of Computer Science and Applications, Sharda School of Computing Science and Engineering, Sharda University, Uttar Pradesh, India, holds 23 years of teaching experience and is pursuing a Ph.D. in computer science and engineering at Shri Venkateshwara University. With an M.E. CSE from Anna University, he has published 8 patents and 10 research papers, specializing in networks, cloud computing, software engineering, and machine learning. He can be contacted at email: rajkumar.jcet@gmail.com.



Dr. Prabu Kaliyaperumal    is an Assistant Professor in the School of Computer Science and Engineering, IILM University, Greater Noida, India, with over 18 years of teaching and research experience. He received his Ph.D. in CSE, M.Tech. in CSE from SRM University, and MBA from Anna University. His research interests include cybersecurity, intrusion detection systems, cloud and edge computing, IoT security, machine learning, deep learning, explainable AI, and network security. He has published 35+ research papers in reputed international journals and conferences, including SCI/SCIE-indexed venues, and holds 10 published patents. He can be contacted at email: mega.prabu@gmail.com.