IAES International Journal of Robotics and Automation (IJRA)
Vol. 15, No. 3, September 2026, pp. 698~708
ISSN: 2722-2586, DOI: 10.11591/ijra.v15i3.pp698-708

Graph-guided contrastive transformer architecture for robust and explainable network intrusion detection

Archana Jayapal[1], Kamalakkannan Somasundaram[2], Arun Kumar Ramamoorthy[3]
[1]Department of Computer Science, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
[2]Department of Computer Applications, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India
[3]Digital Forensics and Cyber Security, University of South Wales, Treforest, United Kingdom

Article Info

Article history:

Received Feb 25, 2026
Revised Jun 5, 2026
Accepted Jul 20, 2026

Keywords:

Contrastive representation learning
Graph-guided learning
Intrusion detection system
Network security
Transformer network

ABSTRACT

Intrusion detection systems (IDS) are very instrumental in protecting contemporary network infrastructures against the ever-advancing cyberattacks. Conventional signature-based and machine learning-enabled IDS solutions frequently have difficulty when it comes to high false-positive rates, inability to flexibly adapt to novel attacks, and the lack of support for complex traffic dynamics. New deep learning architectures have better detection properties, yet are limited by feature overlap, temporality, and lack of extensiveness to generalization in changing network conditions. To overcome these issues, this paper presents a new graph-guided contrastive transformer-based intrusion detection system (GCT-IDS) which aims at improving detection accuracy and robustness and preserving real-time feasibility. The framework combines feature interaction by graph modeling, contrastive representation learning, and a sparse self-attention transformer to effectively learn global traffic relationships and behavioral variations. The CSE-CIC-IDS2018 data is used to test the proposed method in real network conditions.

Corresponding Author:

Kamalakkannan Somasundaram
Department of Computer Applications, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS)
Pallavaram, Chennai
Email: kannan.scs@vistas.ac.in

1. INTRODUCTION

The accelerated growth of digital communication, cloud computing, Internet-of-Things (IoT), and robotic cyber-physical systems (CPS) has significantly increased the complexity and vulnerability of modern network infrastructures. In robotics-driven environments such as autonomous vehicles, industrial robots, and smart healthcare systems, continuous data exchange between sensors, actuators, and control units introduces new attack surfaces. Consequently, cyber threats such as distributed denial of service (DDoS), brute-force attacks, botnets, and infiltration attacks continue to evolve, posing serious risks to data confidentiality, integrity, availability, and operational safety of robotic systems [1]. Intrusion detection systems (IDS) have therefore become essential components in securing robotic and networked environments by enabling continuous monitoring and timely identification of malicious activities [2]. Unlike preventive mechanisms, IDS focus on detecting abnormal or unauthorized behavior post-compromise and initiating appropriate response actions to mitigate potential damage [3].

Early IDS solutions primarily relied on signature-based detection, where traffic patterns are matched against known attack signatures. While effective for known threats, these systems fail to detect zero-day

attacks and require frequent manual updates [4], [5]. Anomaly-based IDS approaches, leveraging statistical techniques and machine learning algorithms such as decision trees, support vector machines, k-nearest neighbors, and random forests, offer improved adaptability. However, they often struggle with high-dimensional data, feature generalization, and class imbalance—challenges that are further amplified in robotics environments with heterogeneous sensor data streams [6], [7].

Recent advancements in deep learning have enhanced IDS capabilities through automated feature extraction and temporal modeling. Models such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), including LSTM and BiLSTM, have shown strong performance in capturing sequential traffic patterns [8]. However, these approaches suffer from high computational overhead, limited interpretability, and sensitivity to noisy or redundant inputs. In robotics applications, where real-time decision-making is critical, such limitations can degrade system responsiveness and reliability. Moreover, recurrent architectures often struggle with long-range dependency modeling in complex, dynamic traffic environments [9]. Traditional feature selection techniques like principal component analysis (PCA), mutual information, and recursive feature elimination reduce dimensionality but fail to capture inter-feature relationships and structural dependencies inherent in robotic communication networks [10], [11].

To address these limitations, this paper proposes a graph-guided contrastive transformer-based intrusion detection system (GCT-IDS) tailored for intelligent and robotic network environments [12]. The proposed framework leverages graph-based modeling to capture structural relationships among features and communication nodes, enabling more context-aware feature representation. Contrastive representation learning is employed to generate robust and discriminative embeddings that enhance generalization to unseen attack patterns, particularly in dynamic robotic systems [13]. Furthermore, a lightweight self-attention transformer is utilized to model global dependencies across traffic flows without relying on computationally expensive recurrent mechanisms. This integrated architecture improves detection accuracy, robustness, scalability, and interpretability, making GCT-IDS highly suitable for securing next-generation robotic and cyber-physical network infrastructures [14], [15].

The remainder of this paper is organized as follows. Section 2 presents a comprehensive review of recent and relevant studies on network IDS, with particular emphasis on machine learning and deep learning–based approaches, highlighting their strengths, limitations, and research gaps. Section 3 describes the proposed graph-guided contrastive transformer–based intrusion detection methodology in detail, including data preprocessing, feature interaction modeling, representation learning, and classification mechanisms. Section 4 discusses the experimental results and performance evaluation of the proposed framework under realistic network conditions. Finally, the paper concludes with key findings and outlines future research directions for further enhancing intrusion detection performance and adaptability.

2. LITERATURE REVIEW

The development of internet usage produced various traffic with signs of numerous cyberattacks. The latest dataset CSE-CIC-IDS2018 was used to apply deep learning methods in intrusion detection with the conventional evaluation metrics. Six models, such as DNN, CNN, RNN, LSTM, CNN + RNN and CNN + LSTM, were built after preprocessing and binary and multi-classical classification and detection of benign traffic and six categories of attacks were performed [16]. The accuracy of all the models was more than 98. DNN, CNN, and RNN models were individually less inference-time-consuming and, therefore, were more applicable in practice when it comes to IDS applications.

Cloud computing facilitated the on-demand-basis availability of network and computer resources such as storage, and data management, and improved the efficiency of the system. However, with these advantages, cloud environments were characterized by huge security issues especially when it comes to securing resources and services. In order to overcome these issues, IDS were embraced to track network traffic and detect abnormal traffic [17]. A random forest and feature engineering-based cloud-based model of intrusion detection was created to enhance the accuracy of detection. In Bot-IoT and NSL-KDD datasets, 98.3% and 99.99 gave the highest accuracy, precision, and recall; thus, indicating high performance.

The Internet of Things also linked physical objects in different fields, including transportation, healthcare, agriculture, and defense, and allowed them to be used in real-time yet posed a serious security threat. Predictive IoT network security was not efficient with traditional signature- and rule-based methods [18]. Pearson correlation coefficient-convolutional neural network model was designed as an IDS to detect network anomalies. The use of important linear features combined with CNN-based learning was used in binary and multiclass attack detection. Testing on NSL-KDD, CICIDS-2017 and IOTID20 databases demonstrated high precision of 99.89 and extremely low misclassification.

The high Internet traffic rates had diversified and complicated malicious attacks and single-modal intrusion detection models had not maximized the rich feature that networks offer, which resulted in poor

performance. This limitation was overcome by proposing a multimodal hybrid parallel network intrusion detection model [19]. Statistical information and raw payload data were used to extract network traffic features through specialist neural architectures. The CNNs learn the spatial-temporal features via CNN-LSTM branches and statistical features via CNNs. CosMargin Feature fusion with a CosMargin classifier obtained 99.98 accuracy on benchmark datasets.

It introduced a new framework of intrusion detection, that is, it was able to detect cyberattacks on the internet of vehicles environment such as DoS, DDoS, DRDoS, brute force, botnets, and sniffing attacks. Network traffic was analyzed by a machine learning based system to identify abnormal flows in the network [20]. The methodology included preprocessing with Z-score normalization, feature selection with a regression approach to reduce the complexity of the algorithms, and trained ensemble models using the random forest and boosting algorithms. Tests on benchmark problems attained more than 99.8 accuracy with low detection latency, which was better than current practices.

3. PROPOSED WORK

The proposed methodology is based on a systematic sequence of work that includes flow-based traffic construction using the CSE-CIC-IDS2018 data. To improve the quality of data and its contextual representation, data cleaning, imputation, normalization, and temporal enrichment are used. Graph-based feature selection finds structurally influential features, which are converted into the latent embeddings through contrastive Siamese learning. A graph-guided sparse transformer optimized by imbalance aware loss functions is used to conduct final intrusion classification which allows accurate and real time detection.

3.1. Dataset description and traffic flow construction

The intrusion detection framework proposed is tested on the CSE-CIC-IDS2018 dataset which is among the most complete and realistic benchmark datasets that exist to conduct research on network intrusion detection [21]. This data was created to represent real-life enterprise network conditions and comprises not only a broad variety of benign traffic but also various types of modern cyber-attacks. It includes more than one million network flow records, all of which have a rich set of traffic related attributes including packet statistics, protocol behavior, and timing information. Diversity and size of the dataset render it especially appropriate to test sophisticated methodologies of intrusion detection in the conditions of real operations.

$$F_i = \{p_j | (s_j, d_j, pr_j) = (s_j, d_j, pr_j), |t_j - t_i| \leq \Delta T\} \quad (1)$$

Where F_i is the i^{th} bidirectional traffic flow, p_j is the packet j; s_j, d_j are source and destination addresses, pr_j is the protocol type, t_j is the packet timestamp and ΔT adaptive time window. As opposed to examining raw packets separately, the proposed solution breaks down network traffic into two-way flow sessions.

3.2. Data cleaning and integrity validation

The quality of data is fundamental to ensuring the success of any IDS, especially in the case of big and heterogeneous network traffic data. The quality of the data contained in the CSE-CIC-IDS2018 dataset can still include unnecessary records, malformed flows or inconsistencies added by data captures and aggregations. In order to resolve these, an effective process in data cleaning and integrity verification concept is employed before being analyzed further. The proposed methodology uses density-based neighborhood validation to determine redundant or anomalous flow records rather than traditional duplicate removal which uses the exact matching of the duplicates. This scheme analyses the local neighborhood structure of traffic flows in the feature space and eliminates recordings that have an abnormally large similarity density which tends to represent duplication artifacts or logging artifacts. Also, flow records containing inconsistent protocol fields, invalid timestamps or invalid attribute values are identified by integrity checks enforced by rules and fixed or eliminated. This validation procedure guarantees that the remainder data is true to the real network activity, so there is less bias and noise does not negatively impact on the subsequent learning phases [22]–[25].

$$\rho(x_i) = \sum_{j=1}^{N} I\left(\left|x_i - x_j\right| \leq \epsilon\right) \quad (2)$$

Where $\rho(x_i)$ is the local density of sample x_i; x_i, x_j are traffic flow feature vectors, ϵ is the neighborhood radius and $I(\cdot)$ is the indicator function.

3.3. Data imputation and feature normalization

The datasets collected by the network traffic are often characterized by the presence of missing or incomplete values because of packet loss, performance constraints of monitoring, or sensor failures. Such records should not be ignored or simplistic imputation strategies should be used to produce a distorted distribution of features and poor performance of models. Where the numerical values are missing in the proposed workflow, a K-nearest neighbors (KNN) based similarity imputation method is used. This technique finds clusters of the traffic flows that share the same behavioral properties and approximates missing values using the local structure of the data, hence maintains the inherent relationships among attributes [26]. After imputation, the normalization of features is undertaken in order to provide numerical stability and uniform accounting of features.

$$\hat{x}_{i,k} = \frac{1}{K}\sum_{j\in N_k(i)} x_{j,k} \tag{3}$$

Where $\hat{x}_{i,k}$ represents the imputed value of feature $k, N_K(i)$ is the set of K nearest neighbors and $x_{j,k}$ is feature k of neighbor j.

$$x^{'} = Q^{-1}\big(F(x)\big) \tag{4}$$

Here, x is the original feature value, $F(x)$ is the empirical cumulative distribution function, $Q^{-1}(\cdot)$ is the inverse target quantile function and x' is the normalized feature. Figure 1 illustrates the architecture of the proposed GCT-IDS framework.

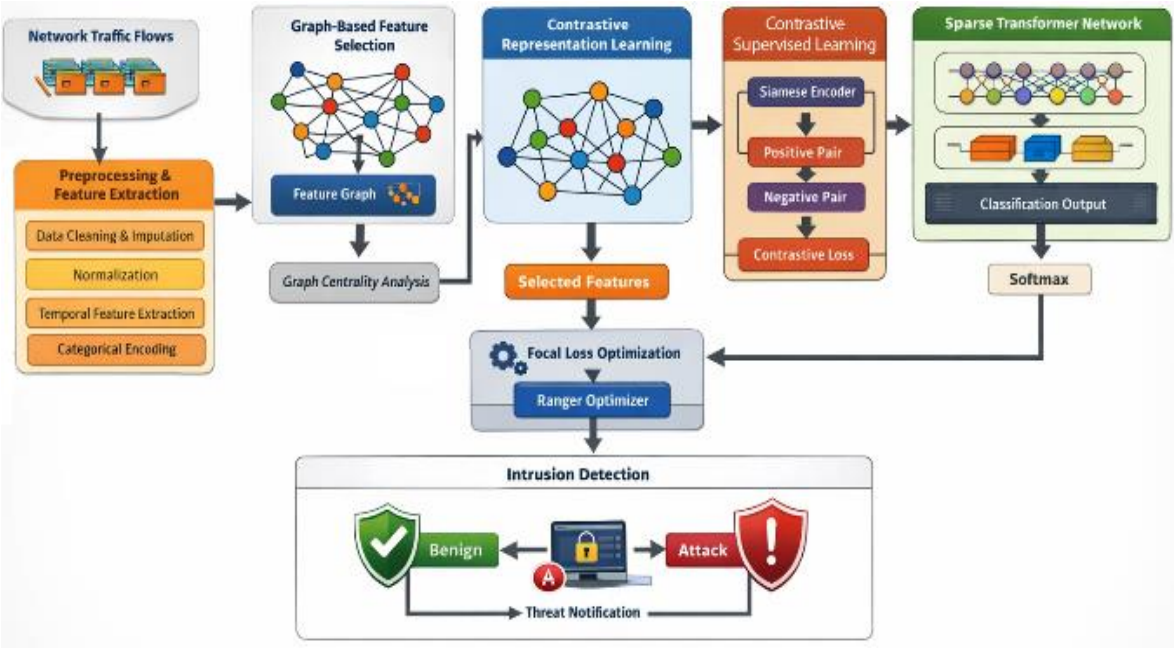

Figure 1. GCT-IDS system architecture

3.4. Feature encoding and temporal enrichment

Some of the categorical attributes in the dataset, *e.g.*, protocol type and service identifiers are not processable directly by learning algorithms. In order to encode these attributes efficiently the suggested methodology applies target-guided statistical encoding. The encoding method substitutes categorical values with statistically obtained estimates depending on their conditional association with the class names and permits the model to record discriminative information with little or no major growth of dimensionality. This method will prevent the sparsity and scalability challenges that one-hot encoding is known to bring in large datasets. In addition to the use of static feature representation, the use of temporal dynamics is important in the separation of benign behavior and the malicious activity for automation. In order to extract these dynamics, the methodology employs temporal enrichment in terms of multi-scale sliding window analysis.

Entropy change, inter-arrival time volatility and burst intensity are temporal descriptors calculated on both short term and long-term windows. These characteristics allow the system to simulate changing traffic patterns and being able to detect subtle time variations linked to reconnaissance, brute force efforts or low rates attacks. Temporal enrichment is a particularly useful approach in contextualizing the network activity, as well as providing better detectability of the intrusion scenarios of a more sophisticated nature.

$$E(c) = E[Y|C = c] \tag{5}$$

$E(c)$ is the encoded value for category c; Y is the class label and C is the categorical feature.

$$H_t = -\sum_{i=1}^{n} p_i \log p_i \tag{6}$$

H_t is the entropy within time window t, p_i is the probability of packet event i and n is the number of events in window.

3.5. Graph-based feature selection

The highly dimensional feature spaces are prone to redundancy and computing inefficiency and therefore reduction can be a very crucial phase of the intrusion detection process. Unlike the relevance-based or elimination-based selection methods, the framework in question uses a graph-based feature selection approach. Here, features are represented as the nodes of a feature interaction graph, features that are statistically dependent on each other illustrated as the edges of the graph.

$$C(v_i) = \sum_{j=1}^{N} A_{ij} \cdot C(v_j) \tag{7}$$

Where $C(v_i)$ is the centrality score of feature node i; A_{ij} is the adjacency matrix and N is the number of features. This graph is analyzed using spectral centrality analysis in order to determine the structural influential features that are central to the entire interaction network. Attributes that have a high centrality are kept, as they play an important role in the general representation of traffic behavior. This graph-based process of selection is not only a dimensionality reduction algorithm but also tends to retain complex relationships between features that are frequently ignored by other selection techniques. Consequently, the chosen feature set is not only small but also informative and, therefore, enhances both computational efficiency and detectability.

3.6. Proposed graph-guided contrastive transformer (GCT-IDS)

The last stage of classification is carried out with the help of the proposed graph-guided contrastive transformer that is known as GCT-IDS. The model combines the benefits of graph-inspired feature selection and contrastive representation learning and the expressivity of transformer-based models. Transformer encoder uses sparse self-attention, and it is able to learn global dependency across traffic embeddings at low computation.

$$Att(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}} \odot M\right)V \tag{8}$$

where Q, K, V are query, key, value matrices, d_k is the key dimension, M is the sparsity mask and $\odot$ is the element-wise multiplication. As opposed to recurrent architectures, the transformer processes embeddings parallel to each other, which means that they can be trained and inferred faster. The attention mechanism is dynamically calculated and weighs varied components of the acquired representations which enables the model to concentrate on most pertinent pattern of behavior in intrusion classification. The Ranger optimizer is used to perform model optimization, and it is a combination of rectified adaptive moment estimation and lookahead strategies to enhance convergence stability. Moreover, focal loss is used in the training process to deal with the problem of the imbalance between classes by focusing on those minority attacks that are difficult to classify. Collectively, the above design decisions can lead to a strong and scalable intrusion detector model that can perform well against dynamic and various threats in the network.

$$L_{focal} = -\alpha\left(1 - p_t\right)^{\gamma} \log\left(p_t\right) \tag{9}$$

where p_t is the predicted probability for true class, α is the class balancing factor, and γ is the focusing parameter.

Algorithm 1. Graph-guided contrastive transformer-based intrusion detection (GCT-IDS)

Input: Raw network traffic packets $P = \{p_1, p_2, \ldots, p_n\}$, time window ΔT, number of neighbors K, graph threshold ϵ, contrastive margin m

Output: Predicted traffic class $\hat{Y} \in \{Benign, Attack\}$

1. Flow Construction: Group packets into bidirectional flows using
$F_i = \{p_j | (s_j, d_j, pr_j) = (s_j, d_j, pr_j), |t_j - t_i| \leq \Delta T\}$

2. For each flow feature vector x_i, compute local density $\rho(x_i) = \sum_{j=1}^{N} I\left(\left||x_i - x_j|\right| \leq \epsilon\right)$
Remove flows with abnormal density.

3. For missing feature k in flow i, estimate using $\hat{x}_{i,k} = \frac{1}{K}\sum_{j \in N_k(i)} x_{j,k}$

4. Apply quantile normalization $x' = Q^{-1}(F(x))$

5. Encode categorical feature C using $E(c) = E[Y|C = c]$

6. Compute entropy over sliding window $H_t = -\sum_{i=1}^{n} p_i \log p_i$

7. Construct feature interaction graph $G(V, E)$
Compute centrality: $C(v_i) = \sum_{j=1}^{N} A_{ij} \cdot C(v_j)$
Select top-central features.

8. Generate embeddings z_i, z_j using Siamese encoder
Optimize contrastive loss $L_{con} = y \cdot d^2 + (1 - y) \cdot \max(0, m - d)^2$

9. Apply sparse self-attention
$Att(Q, K, V) = softmax\left(\frac{QK^T}{\sqrt{d_k}} \odot M\right)V$

10. Compute focal loss: $L_{focal} = -\alpha(1 - p_t)^{\gamma} \log(p_t)$
Update parameters using Ranger optimizer.

11. Assign class label: $\hat{Y} = \arg\max P(Y|F_i)$

Return $\hat{Y}$

End Algorithm

standards.

4. RESULTS AND DISCUSSION

In the proposed GCT-IDS, it is the working principle based around the transformation of raw network traffic into semantically rich representations that can be used to perform accurate and real-time detection of intrusions. To ensure the reliability and robustness of the proposed GCT-IDS model, extensive statistical validation was performed. The entire experimental pipeline, including data preprocessing, stratified data splitting, model training, and evaluation, was executed 10 independent times. In each run, random initialization and data shuffling were applied while maintaining consistent stratified training, validation, and testing splits to ensure fairness and reproducibility.

The performance of the model was evaluated using standard classification metrics, including Accuracy, Precision, Recall, and F1-score. The results of these tests confirm that the performance improvements achieved by GCT-IDS are statistically significant ($p < 0.05$) across all evaluation metrics. This demonstrates that the proposed model consistently outperforms existing approaches and that the improvements are not due to random variation. Figure 2 shows the total detection performance of the proposed GCT-IDS model in various metrics of evaluation. Figure 3 depicts the performance of the suggested GCT-IDS model in terms of the detection of various types of traffic. The findings reveal a high level of precision, recall, and F1-score in both benign and malicious classes that shows a balanced ability in detection. The frequent attack types that the model performed well include DoS, DDoS and PortScan, which indicate that the model was effective in detecting a prevalent pattern of intrusion. The framework itself continues to record good performance of low-frequency and stealthy attacks like infiltration and Slowloris which are typically challenging to trace since they have small behavioral prints.

The rankings of such attacks are slightly lower yet they are still well above the range of acceptable levels which point to strong generalization. This universal behavior in response to the classes may be explained by contrastive representation learning mechanism, which improves discrimination between traffic behaviors, and transformer-based global dependency modeling that incorporates fine variations amid traffic flows. Figure 4 is the comparison between the proposed GCT-IDS and the traditional machine learning model and the deep learning-based intrusion detection models. Classical methods like the logistic regression and decision trees have poor performance because they cannot provide a nonlinear relationship and temporal relationship. Random forest and gradient boosting are ensemble methods that can be used to enhance accuracy, nonetheless, these methods remain insufficient when applied in complex and dynamic traffic patterns. Figure 5 analyses the strength of GCT-IDS to various types of attacks. Detect rate of the proposed framework is always high in terms of brute-force, denial-of-service, scanning, and application-layer attacks, which indicates the flexibility of the proposed framework. It is interesting to note that low rate and stealthy attacks like SQL injection, XSS or slow HTTP attacks have a detection rate of over 97 that most traditional IDS models cannot detect. This strength can be credited to temporal enrichment and contrastive learning that help the system to observe slow and subtle changes of normal behavior.

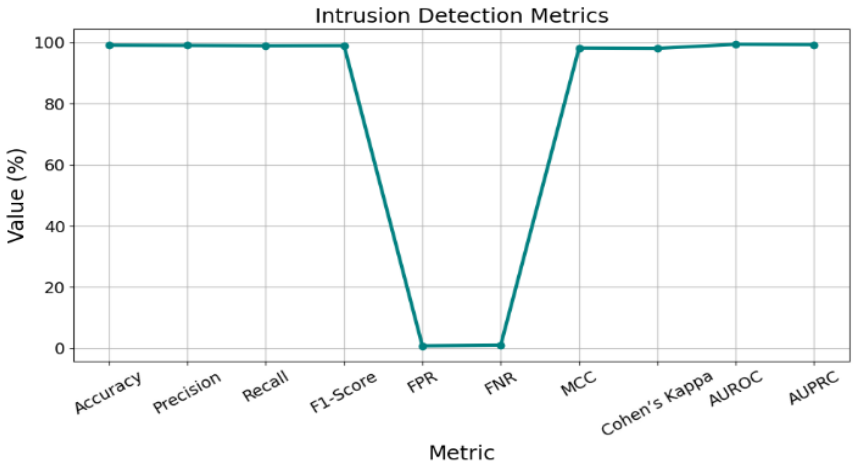

Figure 2. Intrusion detection metrics

Figure 3. Class-wise detection performance metrics

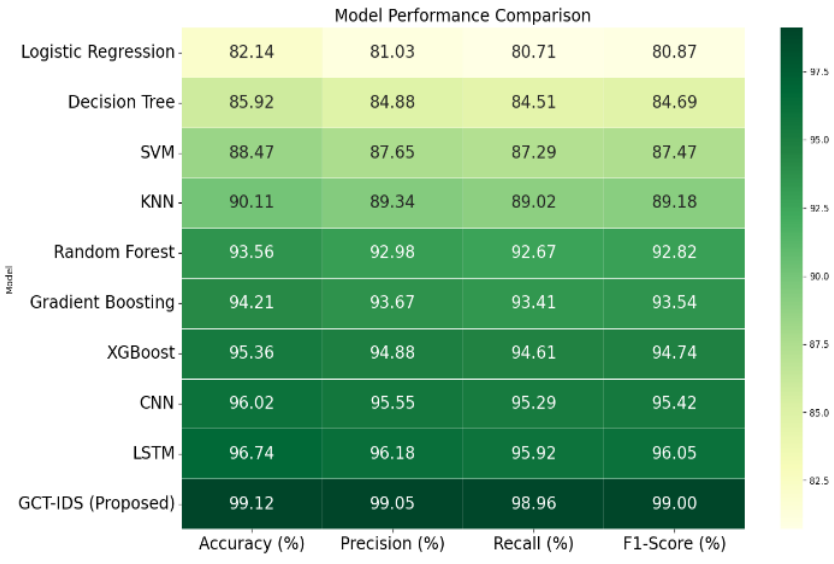

Figure 4. Model performance comparison

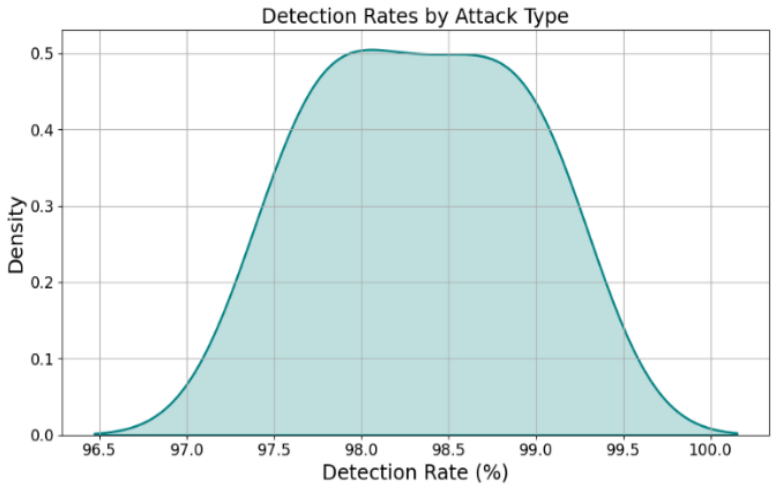

Figure 5. Detection rates by attack type

The fact that the distributed attacks have a high detection rate is yet another indication that the transformer global attention mechanism is able to capture correlated patterns at the traffic flows. In general, Table 1 gives the performance of GCT-IDS in comparison with other machine learning and deep learning models in terms of training time, testing, and memory use. Although the traditional models have lower computational cost, they do not have good detection accuracy. The advanced computational overhead of deep learning models in comparison to simple architectures and processing in a sequence increases the computational overheads.

Table 2 shows the performance of GCT-IDS in terms of temporal generalization in the various time segments and traffic load situations. The model has a high level of accuracy and recall during morning, afternoon, evening, and night times, which is highly temporal stable.

Table 1. Computational performance evaluation

Model	Training Time (s)	Testing Time (s)	Memory Usage (MB)
Random Forest	118	21	640
Gradient Boosting	185	29	710
XGBoost	210	34	820
CNN	265	42	910
LSTM	295	48	980
BiLSTM	322	53	1040
Transformer	308	46	1020
Autoencoder-CNN	280	44	960
Hybrid DL	335	58	1100
GCT-IDS	315	49	1055

Table 2. Temporal generalization performance

Time Segment	Accuracy (%)	Recall (%)
Morning	99.21	99.05
Afternoon	99.08	98.94
Evening	99.12	98.97
Night	98.97	98.83
Weekday	99.15	99.01
Weekend	99.04	98.89
Peak Traffic	98.88	98.71
Off-Peak	99.24	99.12
High Load	98.92	98.76
Low Load	99.31	99.18

5. CONCLUSION

The paper introduced a GCT-IDS which is aimed at overcoming the shortcomings of the current IDS models in managing complex, high-dimensional and changing network traffic. The interaction modeling of graph-based features, contrastive representation learning and sparse self-attention transformers are

incorporated into the proposed framework, which is effectively capable of capturing global dependencies as well as weak anomalies of behavior. An experiment on the CSE-CIC-IDS2018 dataset proves that GCT-IDS performs better than the traditional machine learning and deep learning-based IDS methods in terms of detection accuracy (99.12). The findings affirm that the proposed model provides a solid, scalable and explainable solution to the current network security settings. Its capability to sustain good performance in detection of various forms of attacks and time variation features render it applicable in the real world. The current study can be expanded by future research to include federated learning to promote distributed intrusion detection and privacy-sensitive intrusion detection. The implementation of online learning mechanisms could also increase flexibility to new threats. Also, the framework can be applied in the context of multi-modal security data and edge-based deployment applications, which are prospects in developing the next-generation IDS systems.

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
Archana Jayapal	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	✓
Kamalakkannan Somasundaram	✓		✓	✓	✓			✓	✓		✓	✓	✓	
Arun Kumar Ramamoorthy		✓				✓	✓			✓	✓		✓	

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] I. Mahmoudi, D. E. Boubiche, S. Athmani, H. Toral-Cruz, and F. I. Chan-Puc, "Toward generative AI-based intrusion detection systems for the Internet of Vehicles (IoV)," *Future Internet*, vol. 17, no. 7, p. 310, 2025, doi: 10.3390/fi17070310.

[2] B. Xiang, R. Zheng, K. Zhang, C. Li, and J. Zheng, "FFT-RDNet: A time-frequency-domain-based intrusion detection model for IoT security," *Sensors*, vol. 25, no. 15, p. 4584, 2025, doi: 10.3390/s25154584.

[3] M. M. Mahmoud, Y. O. Youssef, and A. A. Abdel-Hamid, "XI2S-IDS: An explainable intelligent 2-stage intrusion detection system," *Future Internet*, vol. 17, no. 1, p. 25, 2025, doi: 10.3390/fi17010025.

[4] H. Peng, C. Wu, and Y. Xiao, "FD-IDS: Federated learning with knowledge distillation for intrusion detection in non-IID IoT environments," *Sensors*, vol. 25, no. 14, p. 4309, 2025, doi: 10.3390/s25144309.

[5] M. Al Rawajbeh, A. J. Maria Soosai, L. K. Ramasamy, and F. Khan, "Trustworthy adaptive AI for real-time intrusion detection in industrial IoT security," *Internet of Things*, vol. 6, no. 3, p. 53, 2025, doi: 10.3390/iot6030053.

[6] N. Terawi, H. I. Ashqar, O. Darwish, A. Alsobeh, P. Zahariev, and Y. Tashtoush, "Enhanced detection of intrusion detection system in cloud networks using time-aware and deep learning techniques," *Computers*, vol. 14, no. 7, p. 282, 2025, doi: 10.3390/computers14070282.

[7] F. Alserhani, "Intrusion detection and real-time adaptive security in medical IoT using a cyber-physical system design," *Sensors*, vol. 25, no. 15, p. 4720, 2025, doi: 10.3390/s25154720.

[8] E. Alalwany, B. Alsharif, Y. Alotaibi, A. Alfahaid, I. Mahgoub, and M. Ilyas, "Stacking ensemble deep learning for real-time intrusion detection in IoMT environments," *Sensors*, vol. 25, no. 3, p. 624, 2025, doi: 10.3390/s25030624.

[9] A. Alabdulatif, "A novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence," *Applied Sciences (Switzerland)*, vol. 15, no. 14, p. 7984, 2025, doi: 10.3390/app15147984.

[10] M. B. Bankó *et al.*, "Advancements in machine learning-based intrusion detection in IoT: Research trends and challenges," *Algorithms*, vol. 18, no. 4, p. 209, 2025, doi: 10.3390/a18040209.
[11] N. Savanović *et al.*, "Intrusion detection in healthcare 4.0 Internet of Things systems via metaheuristics optimized machine learning," *Sustainability (Switzerland)*, vol. 15, no. 16, p. 12563, 2023, doi: 10.3390/su151612563.
[12] D. Musleh, M. Alotaibi, F. Alhaidari, A. Rahman, and R. M. Mohammad, "Intrusion detection system using feature extraction with machine learning algorithms in IoT," *Journal of Sensor and Actuator Networks*, vol. 12, no. 2, Mar. 2023, doi: 10.3390/jsan12020029.
[13] A. Kumar and J. A. Gutierrez, "Impact of machine learning on intrusion detection systems for the protection of critical infrastructure," *Information (Switzerland)*, vol. 16, no. 7, p. 515, 2025, doi: 10.3390/info16070515.
[14] H. Attou *et al.*, "Towards an intelligent intrusion detection system to detect malicious activities in cloud computing," *Applied Sciences (Switzerland)*, vol. 13, no. 17, p. 9588, 2023, doi: 10.3390/app13179588.
[15] Z. Wang, J. Li, S. Yang, X. Luo, D. Li, and S. Mahmoodi, "A lightweight IoT intrusion detection model based on improved BERT-of-Theseus," *Expert Systems with Applications*, vol. 238, p. 122045, 2024, doi: 10.1016/j.eswa.2023.122045.
[16] Y. C. Wang, Y. C. Houng, H. X. Chen, and S. M. Tseng, "Network anomaly intrusion detection based on deep learning approach," *Sensors*, vol. 23, no. 4, p. 2171, 2023, doi: 10.3390/s23042171.
[17] H. Attou, A. Guezzaz, S. Benkirane, M. Azrour, and Y. Farhaoui, "Cloud-based intrusion detection approach using machine learning techniques," *Big Data Mining and Analytics*, vol. 6, no. 3, pp. 311–320, Sep. 2023, doi: 10.26599/BDMA.2022.9020038.
[18] M. Bhavsar, K. Roy, J. Kelly, and O. Olusola, "Anomaly-based intrusion detection system for IoT application," *Discover Internet of Things*, vol. 3, no. 1, p. 5, 2023, doi: 10.1007/s43926-023-00034-5.
[19] S. Shi, D. Han, and M. Cui, "A multimodal hybrid parallel network intrusion detection model," *Connection Science*, vol. 35, no. 1, 2023, doi: 10.1080/09540091.2023.2227780.
[20] M. S. Korium, M. Saber, A. Beattie, A. Narayanan, S. Sahoo, and P. H. J. Nardelli, "Intrusion detection system for cyberattacks in the Internet of Vehicles environment," *Ad Hoc Networks*, vol. 153, p. 103330, 2024, doi: 10.1016/j.adhoc.2023.103330.
[21] Solarmainframe, "IDS intrusion CSV dataset," *Kaggle*. https://www.kaggle.com/datasets/solarmainframe/ids-intrusion-csv (accessed Jun. 18, 2025).
[22] A. P. Muniyandi *et al.*, "Intelligent security system for preventing DDoS attacks for 6G enabled WBSN using improve grey wolf optimization," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5775–5782, 2024, doi: 10.1109/TCE.2024.3416549.
[23] H. M. Belachew, M. Y. Beyene, A. B. Desta, B. T. Alemu, S. S. Musa, and A. J. Muhammed, "Design a robust DDoS attack detection and mitigation scheme in SDN-edge-IoT by leveraging machine learning," *IEEE Access*, vol. 13, pp. 10194–10214, 2025, doi: 10.1109/ACCESS.2025.3526692.
[24] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018*, 2018. doi: 10.14722/ndss.2018.23204.
[25] Y. Fu, D. Liu, J. Chen, and L. He, "Secretary bird optimization algorithm: a new metaheuristic for solving global optimization problems," *Artificial Intelligence Review*, vol. 57, no. 5, pp. 1–102, 2024, doi: 10.1007/s10462-024-10729-y.
[26] Y. E. Kim, Y. S. Kim, and H. Kim, "Effective feature selection methods to detect IoT DDoS attack in 5G core network," *Sensors*, vol. 22, no. 10, p. 3819, May 2022, doi: 10.3390/s22103819.

BIOGRAPHIES OF AUTHORS

Archana Jayapal research scholar at Vels Institute of Science, Technology, and Advanced Studies, Chennai, Tamil Nadu, India. She has expertise in deep learning intrusion detection systems. She can be contacted at archanaartistryacademy@gmail.com.

Kamalakkannan Somasundaram received his M.Sc. computer science degree from Bharathidasan University, M.Phil. computer science degree from Periyar University, and Ph.D. in computer science from Vels Institute of Science, Technology and Advanced Studies (VISTAS), Tamil Nadu, India. He is currently working as a professor in the Department of Computer Applications, School of Computing Sciences, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, Tamil Nadu, India, which is a well-known university. He has 21 years of teaching experience at both the UG and PG levels. His research interests include big data analytics, cloud computing, and blockchain technology. He has produced thirteen Ph.D. research scholars. He has published more than 90 research articles in various international journals such as SCI, WOS, Scopus, and UGC-referred journals. He has published 10 patents. He is a reviewer for various journals. He is serving as a co-principal investigator in a Department of Science and Technology (DST) sponsored project. He received the best young scientist award, best faculty award, and best research supervisor award. He can be contacted at kannan.scs@vistas.ac.in.

Arun Kumar Ramamoorthy is a distinguished lecturer in digital forensics and cyber security at the University of South Wales, Treforest, United Kingdom. He holds a B.Eng. in computer science and engineering from Karunya University, Coimbatore, an M.Tech. in information technology, and a Ph.D. from Anna University, Chennai. With 16 years of academic experience, he has made significant contributions to the field of information technology, authoring over 25 research articles in various domains. His areas of expertise include information security, digital forensics, mobile application security, artificial intelligence, machine learning, deep learning, and network security. Dr. Arun is an inventor with two Indian patents in neural networks and machine learning, as well as an Australian patent in cyber security. He is actively involved in professional organizations, being a member of the Computer Society of India (CSI) and the Indian Society for Technical Education (ISTE). He can be contacted at arun.kumar@southwales.ac.uk.