SCALED-IDS: A Deep Semantic Class-Aware Layered Framework for Multiclass Intrusion Detection in Cloud-IoT Environments

Ramya K. M.
REVA University, Bangalore, India | B.M.S. College of Engineering, Bull Temple Road, Bengaluru - 560019, KA, India
kmramya6@gmail.com (corresponding author)

Rajashekhar C. Biradar
REVA University, Bangalore, India
rcbiradar@reva.edu.in

Received: 26 May 2025 | Revised: 17 July 2025 | Accepted: 27 July 2025

 DOI: https://doi.org/10.48084/etasr.12379

ABSTRACT

The growing adoption of cloud-enabled Internet of Things (IoT) systems has introduced new layers of complexity and vulnerability in network security. With billions of interconnected devices generating vast amounts of traffic, traditional Intrusion Detection Systems (IDSs) often fall short, particularly when tasked with identifying diverse and evolving attack types in real time. Existing solutions, whether rule-based or machine learning-driven, struggle with issues such as class imbalance, limited adaptability, and reduced accuracy when exposed to high-dimensional and dynamic data streams. To address these challenges, this paper presents SCALED-IDS, a deep learning-based framework specifically designed for multiclass intrusion detection in cloud-integrated IoT environments. The proposed model introduces a modular architecture that combines semantic understanding and class-aware learning. At its core, the Multi-Stage Attention Representation Extractor (MARE) captures semantic relationships within network traffic using multi-head attention mechanisms. This is followed by Class-Aware Focused Embeddings (CAFE), which guide the decoding process based on class-specific characteristics, improving the detection of rare or underrepresented attack types. The Class-Level Attention Decoder (CLAD) further enhances performance by breaking down the classification task into progressive layers, refining decisions across dominant and minority classes. The effectiveness of SCALED-IDS is demonstrated through experiments on two publicly available datasets, BoT-IoT and CIC-IoT 2023. The results show that the proposed model consistently outperforms existing methods in terms of accuracy, F1-score, and recall, particularly in identifying complex and low-frequency attack classes.

Keywords-multiclass intrusion detection; cloud-IoT environments; deep learning framework; Multi-stage Attention Representation Extractor (MARE); Class-Aware Focused Embeddings (CAFE)

I. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has resulted in the deployment of a vast number of smart devices capable of autonomous communication, requiring minimal human intervention [1]. By 2022, the global count of IoT devices was projected to exceed 46 billion [2]. This exponential growth has led to the development of intelligent cloud-integrated applications across various domains, including residential systems, industrial automation, healthcare, and education. IoT extends the reach of the Internet beyond traditional computing platforms, facilitating interaction with real-world environments through interconnected networks of sensors and actuators. In such systems, end-users and embedded devices are seamlessly integrated into the network to enable real-time data acquisition, control, and bidirectional communication [3]. However, this pervasive interconnectivity also creates a significantly enlarged attack surface, making these systems highly susceptible to rapidly propagating cyber threats.

In this context, the protection of cloud-based IoT infrastructures has emerged as a pressing concern, as security and privacy breaches can lead to severe operational, economic, and societal consequences [1]. With the increasing complexity and distributed nature of cloud-IoT networks, there is a growing demand for intelligent, adaptive, and scalable security frameworks [2]. Intrusion Detection Systems (IDSs) play a vital role in this landscape, offering continuous monitoring of network traffic to identify unauthorized access attempts and anomalous behavior [3-5]. IDS solutions are commonly

employed to detect a variety of cyber threats, including Denial of Service (DoS) attacks [6-7], malware, viruses, and unauthorized intrusions [8].

Ensuring intrusion detection in IoT environments requires the fulfillment of sophisticated security requirements, especially in cloud-integrated deployments that must protect against a wide spectrum of attack types [4]. The conventional security objectives of Confidentiality, Integrity, and Availability (CIA) are no longer sufficient in such environments, as cloud-IoT systems introduce novel vulnerabilities and attack vectors [5]. Modern security frameworks must now incorporate additional principles such as privacy, accountability, trust, and auditability. Traditional cybersecurity mechanisms—including antivirus tools, data encryption, authentication protocols, firewalls, and rule-based IDSs—struggle to manage the scale and diversity of contemporary IoT traffic [9]. Although IoT continues to be a transformative technological development, its rapid growth has also escalated the risk of cyberattacks. In cloud-enabled infrastructures with billions of interconnected devices, each node can act as a potential entry point for malicious actors, thereby increasing the likelihood of unauthorized access, data breaches, and service disruption.

This expansion of the cloud-IoT ecosystem is expected to catalyze a corresponding increase in sophisticated cyberattacks [5], necessitating the deployment of real-time intelligent detection mechanisms to mitigate potential damage. Cybercriminals continue to evolve their techniques to exploit vulnerabilities in large-scale cloud-based IoT infrastructures. Although manual approaches offer some level of protection, they are inherently constrained by time, resource limitations, human errors, and lack of scalability, which can severely compromise the performance, reliability, and security of cloud-connected IoT systems. To address these challenges, Artificial Intelligence (AI)-based techniques have emerged as a powerful alternative, providing automation, adaptability, and enhanced detection capabilities. In particular, Deep Learning (DL) models are increasingly utilized to identify and classify cyberattacks within IoT environments, as they are capable of processing vast volumes of traffic data, detecting complex patterns, and adapting to evolving threat behaviors [2, 3]. Their proficiency in uncovering subtle anomalies further enhances the performance of intrusion detection systems in real-world deployments. Consequently, the development of AI-based IDS frameworks has gained significant traction in recent research, especially for addressing the limitations of traditional methods in protecting cloud-integrated IoT infrastructures against multiclass cyberattacks.

Machine Learning (ML) techniques have also been extensively explored for intrusion detection in cloud-enabled IoT environments. Models such as Support Vector Machines (SVM) are commonly applied to identify adversarial activity and restrict the injection of malicious data into network traffic [3]. Other ML classifiers, including Random Forest (RF), Decision Tree (DT), K-Nearest Neighbor (KNN), and XGBoost, have also been utilized for attack detection. These models are often iteratively evaluated using a dynamic set of 30 to 40 features to determine the optimal feature subset for accuracy enhancement. Although certain models, such as XGBoost and ANOVA, demonstrated improved performance under constrained conditions, studies have shown that XGBoost's accuracy declined significantly, from 98% to 64%, when the number of input features increased from 20 to 30 [4]. Similarly, conventional ML approaches, including Logistic Regression (LR), DT, SVM, RF, and Multi-Layer Perceptron (MLP) [5], have been employed to detect Distributed Denial-of-Service (DDoS) attacks in IoT networks. Among these, RF has achieved superior results in terms of reduced false positives and lower computational overhead. However, while ML classifiers have yielded high accuracy for binary classification in controlled environments, their performance in multiclass classification tasks often remains limited. This restricts their effectiveness in real-world cloud-IoT scenarios, where detecting both major and minor attack categories is critical. Several studies have also deployed XGBoost and RF for multiclass attack detection, optimizing model performance through hyperparameter tuning and kernel scaling [6]. However, in comparative evaluations, XGBoost achieved an accuracy of only 89%, which was lower than other competing models.

More recent research has attempted to improve performance by integrating ML classifiers with DL methods, aiming to enhance both binary and multiclass classification of normal versus anomalous traffic. These hybrid systems have employed algorithms such as RF, KNN, LR, Naive Bayes (NB), and Artificial Neural Networks (ANN), using benchmark datasets, such as BoT-IoT and TON-IoT, which typically include a limited feature set of around 15 attributes [7]. Although ML-based methods have demonstrated promise in specific use cases, their generalizability in highly variable and complex cloud-IoT traffic remains limited. As a result, there is an increasing need to shift toward end-to-end DL architectures capable of autonomously learning semantic relationships, adapting to evolving attack patterns, and effectively handling class imbalance in multiclass detection scenarios.

The unprecedented growth of cloud-integrated IoT ecosystems has drastically increased the attack surface for modern cyber adversaries. These environments are characterized by highly heterogeneous device infrastructures, massive data volumes, and dynamic communication patterns, all of which pose substantial challenges to traditional security mechanisms. Conventional IDSs, including signature-based and rule-driven approaches, often fail to provide reliable protection against sophisticated and evolving attack vectors. Existing ML-based IDS models suffer from limited scalability, high false positive rates, and poor generalization to previously unseen or underrepresented attack types—particularly in multiclass intrusion scenarios, where rare threats are frequently overlooked. The complexity intensifies in cloud-enabled IoT environments, where the detection of diverse attack categories, including DoS, reconnaissance, botnets, data exfiltration, and privilege escalation, requires real-time, adaptive, and semantically aware decision-making capabilities. In addition, the high dimensionality and imbalance of IoT network traffic make it difficult for traditional classifiers to capture latent relationships and contextual behaviors associated with different threat classes. These limitations highlight the pressing need for

an intelligent, modular, and class-aware intrusion detection framework that can operate effectively under the constraints of cloud-centric IoT systems.

Motivations and contributions to secure cloud-integrated IoT environments have become increasingly critical due to their expanding attack surface and susceptibility to a wide range of cyber threats. Vulnerabilities in these systems can significantly degrade performance, compromise data integrity, and disrupt service continuity. The diversity of connected devices, the volume of data traffic, and the real-time communication requirements create significant challenges for intrusion detection. Manual and rule-based techniques, although historically useful, are insufficient to handle the dynamic, large-scale, and heterogeneous nature of modern IoT networks. AI-based intrusion detection approaches have emerged as effective alternatives, capable of automating threat detection and learning complex patterns from high-dimensional data. However, existing AI-based IDS models face several limitations, including low classification accuracy, poor detection of minority attack classes, limited multiclass generalization, high computational overhead, and risks of over- or underfitting. These limitations are particularly problematic in cloud-enabled IoT systems, where attack detection must be both scalable and semantically precise. Most current models cannot contextually differentiate between diverse attack patterns or adaptively prioritize rare but critical intrusions. To address this gap, there is a need to design a DL-based IDS that not only scales with the complexity of cloud-integrated traffic but also enhances the detection of minority and multiclass attacks through semantic representation, attention-guided learning, and hierarchical decoding strategies.

This gap motivated the development of a robust, modular, DL-based framework, called SCALED-IDS (Semantic Class-Aware Layered Embedding Decoder for Intrusion Detection Systems), to enable accurate, class-aware, and real-time multiclass attack detection in cloud-IoT environments. Using semantic representation learning and layered decoding strategies, the SCALED-IDS architecture aims to overcome existing shortcomings and improve the reliability and adaptability of modern IDS systems. The proposed SCALED-IDS model involves:

- MARE for semantic representation learning: A transformer-inspired encoder (MARE) is used to autonomously learn deep semantic relationships in IoT traffic using multi-head self-attention, eliminating the need for manual feature engineering.
- Class-Aware Embedding with CAFE: Introduces Class-Aware Focused Embeddings (CAFE), which encode attack-specific semantics to guide attention during decoding, effectively addressing class imbalance and improving minority class detection.
- Hierarchical Decoding with CLAD: Implements a layered Class-Level Attention Decoder (CLAD) that refines predictions through a split-and-conquer approach, enhancing multiclass classification performance and interpretability.

II. RELATED WORK

In traditional ML-based Network IDSs (NIDSs), the process typically begins with feature engineering, where relevant attributes are extracted from raw network traffic, followed by the application of shallow classifiers. Numerous ML techniques, such as KNN, SVM, NB, and DT, have been applied in this context. In [8], a two-stage IDS approach combined SVM with a density-based clustering algorithm to improve classification. In [9], a Naive Bayes model was employed to process raw data, enabling improved feature separation and higher-quality data representation. In [10], an Explainable AI (XAI) approach used a DT model to enhance trust and interpretability within IDSs. However, although these models offer certain advantages, they heavily rely on handcrafted features. Designing and selecting appropriate features requires extensive domain knowledge and manual effort, which significantly limits their scalability and adaptability in complex environments.

More recent research has explored graph-based learning approaches to improve detection performance. The E-graphSAGE framework [11] reformulated the NIDS problem as an edge classification task, where node representations are learned by aggregating edge features from sample neighborhood nodes. Although it simultaneously utilized topological and flow-based information, the process of mapping original IP addresses to randomized ones disrupts the spatial distribution of traffic, potentially affecting the model's reliability. To address these shortcomings, in [12], residual learning was introduced into the E-graphSAGE architecture, preserving the original graph structure and improving the detection of minority attack classes. Recognizing the challenge of limited labeled data in large-scale IoT deployments, recent studies incorporated temporal correlation among network flows. For instance, in [13], an interval-constrained traffic graph was developed, in which structural representations were enriched using a topology-adaptive Graph Convolutional Network (GCN). Similarly, in [14], a dynamic line graph neural network was proposed to model spatiotemporal dependencies and extract structural information from historical IP interaction snapshots. However, despite these advances, existing supervised learning methods are constrained by their dependence on large volumes of labeled data, which limits their effectiveness in detecting previously unseen or evolving attack patterns and hinders scalability in real-world cloud-enabled IoT environments.

Recent research has focused on improving Graph Neural Network (GNN)-based NIDS frameworks in scenarios where only a few-shot labeled samples are available. In [15], flow graph features were extracted using a subgraph topology constructed from a limited number of initial interactive packets, enabling fast and accurate intrusion detection with minimal supervision. In [16], a predictive self-supervised learning approach was introduced through the TS-IDS framework, which enriched node embeddings by categorizing endpoint nodes based on the volume of traversing traffic. These strategies demonstrated improved detection performance under data-scarce conditions. Building on this direction, a label-aware graph contrastive learning framework was proposed to address

the dual challenges of few-shot learning and class imbalance in NIDS. This approach leveraged structural similarity and semantic alignment within the graph space to better generalize across underrepresented attack types.

In addition to graph-based strategies, lightweight DL models have also been explored for real-time intrusion detection in constrained environments. The method described in [17] utilized refined Controller Area Network (CAN) traffic features and a compact 1D DL network. Key features, including time interval series, message IDs, and CAN payloads, were extracted using a T-shaped windowing mechanism, vectorized, and passed through an efficient 1D convolutional architecture for classification. This design demonstrated strong performance in both binary and multiclass classification tasks on publicly available datasets, validating the efficacy of feature refinement and lightweight convolutional modeling in practical detection scenarios.

Further advances in intrusion detection for IoT networks have explored hybrid DL and metaheuristic optimization strategies. In [18], a distributed multiclass detection framework employed Golden Jackal Optimization (GJO) in conjunction with a DL model (DMCD-GJODL). This approach applied min–max scaling for input normalization and utilized a Chaotic Crow Search Optimization Algorithm (CSSOA) for feature selection. Classification was performed using a Bi-Directional Gated Recurrent Unit (BiGRU), optimized using the GJO algorithm, enhancing detection accuracy and efficiency.

Transformer-based architectures have also gained attention for their ability to detect sophisticated and dynamic threats through self-attention mechanisms. In [19], an attention-driven transformer model was proposed for intrusion detection, offering an adaptable and robust framework capable of handling evolving threat behaviors in network traffic. In addition, transfer learning has been investigated as a means of improving model robustness in environments with limited labeled data. A robustness-preserving framework, named Contrastive Adversarial Representation Distillation (CARD) [20], facilitated the transfer of knowledge from a robust source model to a target model. CARD addressed critical challenges, including data scarcity in the target domain, cross-domain differences, and the need for resilience against both evading attacks and natural data corruptions.

III. PROPOSED METHOD

Traditional IDSs, whether rule-based or ML-driven, have demonstrated limited effectiveness in managing the evolving threat landscape within cloud-integrated IoT environments. Classical ML techniques, such as SVM, RF, or KNN, are heavily based on manual feature engineering and struggle to generalize across diverse attack types—particularly in multiclass intrusion scenarios characterized by class imbalance and suppression of minority classes. Even recent DL models often adopt flat classification schemes and lack semantic awareness, leading to reduced accuracy, poor interpretability, and suboptimal performance under cloud-scale data volumes. Moreover, most existing IDS frameworks are not architecturally designed to operate under the unique constraints of cloud-enabled IoT infrastructures, which include high traffic speed and volume, heterogeneous device communication patterns, low-latency detection requirements, and frequent exposure to unseen or zero-day attack vectors.

In such environments, where intrusion incidents can jeopardize critical infrastructure, such as medical systems or industrial control networks, there is a pressing need for an IDS solution that is not only accurate but also adaptive, semantically aware, and robust across multiple attack classes. To address these limitations, this study proposes SCALED-IDS, a novel modular DL framework built specifically for multiclass cyberattack detection in cloud-centric IoT systems.

A. Preliminaries and Data Preprocessing

SCALED-IDS comprises four phases that include preprocessing and encoder layers, including MARE, CLAD, and CLSFFN classifiers. Figure 1 shows the framework of the SCALED-IDS model.

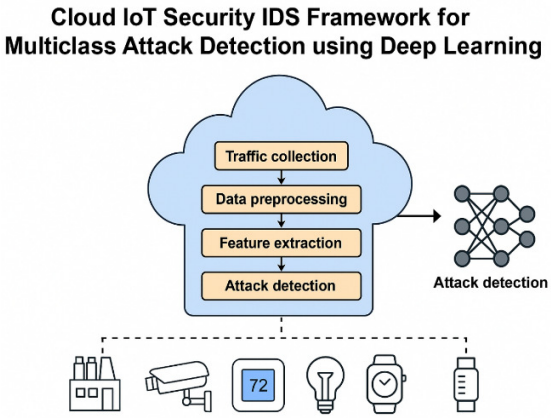

Fig. 1. Cloud IoT multiclass IDS.

Traffic attributes are passed to the encoder layers to obtain a new attribute expression. The output of the encoder and the CAFE are stored in the decoder. The decoder is developed for progressive classification of threats, starting with the larger classes and later aimed at the minor classes. Finally, the CLS-FFN (Classification Feedforward Network) is implemented to identify particular threat classes. In preprocessing, the first phase includes a Feature Encoding Component (FEC). The traffic information includes numerical and text attributes. The numerical attributes are converted into floating-point variables, whereas textual attributes are encoded as numerical scores using methods such as one-hot encoding. Missing text attributes are generally neglected. The second preprocessing phase involves a Feature Rescaling System (FRS). Specifically, Gaussian FRS is implemented to ensure that the attributes have the same numerical range. Assume a sample for traffic $z_p \in \mathbb{T}^h$, $p = 1,2,\dots,P$, where h expresses the initial count of attributes and P denotes the count of traffic samples. Eliminating the missing attributes, the attribute dimension becomes f_h. Furthermore, every attribute is then extended into f dimensions. Therefore, every sample is converted into a matrix $Z \in \mathbb{T}^{f_h \times f}$ through linear projections that are used as input for the encoder.

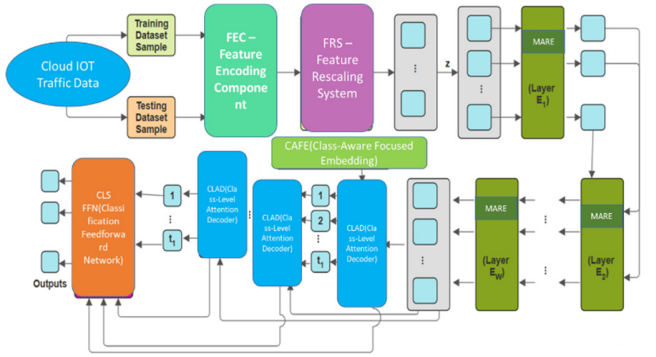

Fig. 2. SCALED-IDS framework.

In preprocessing, it is essential to divide the dataset. Examining the distribution of threats for the training dataset, each layer of split decision for the decoder is used to determine which of the threats can be detected. Initially, anomaly detection is executed for the majority class. However, all threat classes are sorted progressively using every layer, whereas the minority class is dealt with in the concluding layer.

B. Multi-Stage Attention Representation Extractor (MARE)

The input traffic samples are processed through the proposed MARE, which utilizes stacked self-attention mechanisms to derive context-aware embeddings that capture intricate correlations among the IoT traffic features. While considering attribute extraction for traffic using the encoder, only a transformer-encoder model is implemented. The main aim of the model is to use a self-attention technique that allows capturing all the dependencies in pairs between the attributes. For a mapping of traffic data samples into a matrix pattern of $Z \in \mathbb{T}^{f_h \times f}$ as input, the output of the self-attention scheme is:

$$SA(Z) = C(Z)ZY_X \quad (1)$$

where:

$$C(Z) = softmax\left((f)^{-1/2} ZY_S Y_M^V Z^V\right) \quad (2)$$

In (1) and (2), self-attention is expressed as SA, and trainable variables are denoted as Y_S, Y_M, and Y_X for query, key, and score, respectively.

Every layer of the encoder includes a multi-head attention sub-block for various self-attention models and a CLS-FFN sub-block for a feedforward network. The encoder at a y layer produces the output Z_y as a function of Z_{y-1}:

$$Z_y = G_y\left(Z_{y-1}\right), \text{where } y = 1,2,\dots,Y \quad (3)$$

Here, Z_y expresses the y^{th} layer of the encoder and Z_0 is equivalent to Z. After the Y layers of the encoder, the output is summarized inside the deep attribute representation that is expressed as Z_Y.

C. Class-Aware Focused Embeddings (CAFEs)

The CAFE approach introduces a set of trainable, semantically focused vector embeddings aligned with individual threat classes. These embeddings function as class-level attention initiators that guide the decoder toward threat-specific feature extraction via cross-attention over the encoder outputs from MARE. The transformer encoder mentioned above is unable to detect threat classes that represent minorities. To resolve this issue, CAFE is implemented to improve threat awareness. Each threat is related to a particular class query that is used as an attribute input for the decoder. As each query can be learnt, the class data is embedded gradually in the query at the time of training, such that the query is informed of the threat class. Instead of the query being updated from Z along with self-attention from (2), the updates of cross-attention are used to predefine the CAFE vectors that can be learnt, denoted as S, as:

$$D(Z,S) = softmax\left((f)^{-1/2} SY_S Y_M^V Z^V\right) \quad (4)$$

Here, the outputs for cross-attention are given as,

$$CA(Z,S) = D(Z,S)\, ZY_X \quad (5)$$

where CA denotes cross-attention. The output for the cross-attention is managed by S. A transformer-decoder layer is introduced after concatenating the multi-head attention sub-blocks of various models. The initial query input for the decoder is denoted as $S_0 \in \mathbb{T}^{E \times f}$, initialized at random, and the count of threat classes is expressed as E. The input for the a^{th} layer is S_{a-1}, where $a = 1,2,\dots,A$, and the complete count of decoder layers is given as A.

This approach has several advantages. Initially, the output adaptability characteristic of the encoder can be improved. In addition, the CAFE vectors concerning the decoder are trained for multi-class categorization and adjusted to enlighten the particular class data at the time of testing, hence improving the threat awareness.

D. Class-Level Attention Decoder (CLAD)

CAFÉ observation states are used to improve threat-awareness, although they do not resolve the imbalance in the class. To resolve this issue, the CLAD technique is introduced to decompose the single-phase categorization into a multiple-level sub-categorization issue. The divide and conquer method allows the model to redefine its aim progressively toward a particular threat or a specific subset of threats, therefore modelling the distribution of classes definitively. The CLAD mechanism has dual inputs and a single output. One of the inputs is the output of the encoder, which is denoted as Z_Y, and the other is the CAFE of threat-awareness. Each CLAD mechanism is developed utilizing a transformer-decoder layer and a splitting layer. Inside every split layer, a decision initially separates the CAFE related to the threats for detection, and a rearranging layer is used to realign the CAFEs. In addition, an average layer is combined with the CAFEs that remain in an individual query. Finally, a CLS-FFN is used to determine if the query belongs to the subset of the threat classes. If not, then the remaining CAFE would move further to the following decoder layer.

For the advancement of CAFE inside the a^{th} layer of the decoder, initially, the query input S_{a-1} and the output of the encoder Z_Y, are used for the generation of S'_{a-1} given as:

$$S'_{a-1} = F_a(S_{a-1}, Z_Y) \text{ where } a = 1,2,\dots,A \quad (6)$$

Here, F_a is used to denote the operation function for the a^{th} decoder layer, and S'_{a-1} has a t_{a-1} CAFEs. Specifically, the decoder based on the CLAD mechanism is used to split the t_{a-1} CAFEs as u_a and t_a CAFEs, such that the summation of these CAFEs is equivalent to t_{a-1}. The division of the CAFE $S^u_{a-1} \in \mathbb{T}^{u_a \times f}$ relating to u_a threat classes and the t_a CAFEs that are remaining are averaged and collected into an individual query that showcases the additional $(u_a + 1)^{\text{th}}$ class. Similarly, the first classification of the t_{a-1} class is formulated again as a $(u_a + 1)$ class categorization issue, expressed as:

$$\hat{x}_a = classifier([S^u_{a-1}, average(S_a)]) \quad (7)$$

$$S_a = S'_{a-1} - S^u_{a-1} \quad (8)$$

where the average query that is computed is denoted as $average$, $\hat{x}_a$ denotes the logits output at the a^{th} layer of the decoder, and $classifier$ denotes a CLS-FFN classifier. This transformation can be described as:

$$K: \mathbb{T}^{(u_a+1)\times f} \rightarrow \mathbb{T}^{(u_a+1)} \quad (9)$$

Therefore, at the a^{th} layer of the decoder, the integration of the u_a classes are classified as this layer. In other terms, a data sample is categorized in the $(u_a + 1)$ class, then transformed to the $(a + 1)^{\text{th}}$ decoder layer, and is constantly in interaction with S_a for the identification of the threat class. This process of the decoder is iterated for every data sample unless the class is identified.

```
Algorithm 1: SCALED-IDS
Input: Training data set D_training =
  {(z_1, x_1), ..., (z_P, x_P)}, Encoder Y, Decoder A
Output: Model variables ω, CAFEs that are
  learnt: S_0
1:  Initialization of ω and S_0 at random
2:  For p = 1 to P
3:    Data sample for every pair of (z_P, x_P)
      from D_training
4:    Preprocessing z → Z
5:    For y = 1 to Y
6:      Computation of Z_y using (3)
7:    End For
8:    Utilize Z_Y and S_0 as the input for
      the decoder
9:    For a = 1 to A
10:     Calculate x̂_a using (6) and (7)
11:     If the resulting output has a
        detection
12:       Break
13:     End if
14:   End For
15:   Computation of the loss function
      Loss(X, X̂) using(9)
16:   Update ω and S_0 using
      backpropagation
17: End for
18: Return ω and S_0
```

The proposed SCALED-IDS gains a data sample pair (z_P, x_P), $p = 1,2, \ldots, P$ as input, where the class label is expressed as x_P. The information is stored in the encoder Y −layer for the generation of Z_Y. Transferring Z_Y and the first CAFE S_0 in the A-layer decoder, the logits $\hat{x}$ prediction results. The loss function used is:

$$Loss(X, \hat{x}) = \sum_{p=1}^{P} Loss(x_0, \hat{x}_a) = -\sum_{p=1}^{P} x_0 \log \hat{x}_a \quad (10)$$

After training the SCALED-IDS model, the testing phase can be initiated against intrusion networks.

E. Performance Evaluation

The proposed SCALED-IDS model was evaluated on two well-known benchmark datasets, BoT-IoT [21-24] and CIC-IoT 2023 [25]. These datasets were selected for their thorough coverage of normal and malicious IoT network traffic, reflecting both balanced and unbalanced class distributions. The performance of the proposed model was evaluated using accuracy, precision, recall, F1-score, and AUC. In addition, a comparative study was conducted against current state-of-the-art techniques. The results from both datasets confirmed the model's capacity to detect various intrusion types and showed its appropriateness for various IoT intrusion detection mechanisms.

F. Dataset Details

BoT-IoT [21-24] is a well-structured and diverse multi-class dataset, designed to facilitate research on intrusion detection and cybersecurity within IoT environments. It comprises a total of 2,056 instances that are classified into six distinct categories, reflecting a wide range of normal and malicious activities commonly observed in IoT networks. Specifically, the dataset includes 500 instances each for DDoS, DoS, and Reconnaissance (Recon) attacks, which are among the most prevalent and disruptive forms of network threats. These classes are evenly distributed, providing a balanced foundation for training classification models and ensuring robust detection performance across different types of attacks. In addition to these, the dataset includes a significantly smaller number of Theft instances (79), which introduces class imbalance and adds a layer of complexity to the classification task, challenging models to maintain high sensitivity and precision for rare attack types. The Normal class, which represents legitimate traffic, contains 477 instances and is critical to distinguishing benign behavior from anomalies. Its comprehensive composition allows for the development and evaluation of ML and DL algorithms aimed at multiclass intrusion detection. By simulating real-world IoT traffic scenarios with both frequent and infrequent attack patterns, the BoT-IoT multiclass dataset serves as a valuable benchmark for researchers and practitioners working to enhance the security and resilience of IoT systems against evolving cyber threats.

CIC-IoT 2023 [25] is a contemporary and richly annotated benchmark dataset curated to evaluate IDSs in IoT networks, as it captures a comprehensive and realistic mixture of benign and malicious traffic representative of modern IoT environments. The dataset includes a wide spectrum of attack vectors, such as DDoS, DoS, Recon, data theft, spoofing, injection, and other

sophisticated network attacks that target the vulnerabilities inherent in IoT systems. Each sample is carefully labeled, and traffic was collected from a diverse set of IoT devices and applications, making it highly relevant for both academic research and industrial applications. What distinguishes CIC-IoT 2023 is its high-dimensional feature space with rich metadata, which includes flow-based features, packet-level attributes, and time-based statistics, allowing researchers to explore both traditional ML and DL approaches for network traffic classification and anomaly detection. The dataset is well-suited for multiclass classification tasks and enables the benchmarking of models against class imbalance. Its up-to-date nature ensures that it reflects current attack trends and emerging threats in the IoT landscape, making it a valuable resource for developing intelligent, adaptive, and explainable IDS frameworks.

IV. RESULTS

The proposed model was evaluated and compared with [26, 27], using [28] for dimensionality reduction, on the CC-IoT dataset, and the model in [29] on the CC-IoT dataset. Table I presents a comparative performance analysis.

TABLE I. COMPARISON WITH EXISTING METHODS ON CIC-IOT 2023

Class	Accuracy (Existing)	Accuracy (Proposed)	Precision (Existing)	Precision (Proposed)	F1-score (Existing)	F1-score (Proposed)
Benign	95.18	97.80	91.05	96.20	93.07	96.90
DDoS	99.83	99.95	99.82	99.96	99.82	99.96
DoS	99.69	99.92	99.62	99.93	99.66	99.94
Recon	79.21	91.40	84.78	92.80	81.90	92.10
WebB.	36.59	85.30	66.67	87.50	47.24	86.10
BruteF	22.95	81.10	63.64	85.40	33.74	83.20
Spo.	82.60	93.20	84.45	94.00	83.52	93.60
Mirai	99.90	99.97	99.93	99.98	99.92	99.98
Overall	97.62	98.95	97.55	98.90	97.56	98.92

Figure 3 illustrates an overall Accuracy, Precision, and F1-score comparison on the CIC-IoT 2023 dataset. The proposed model demonstrates a consistent improvement in all metrics, with Accuracy increasing from 97.62% to 98.95%, Precision from 97.55% to 98.90%, and F1-score from 97.56% to 98.92%. These results confirm the robustness of the proposed layered architecture in handling complex IoT traffic patterns.

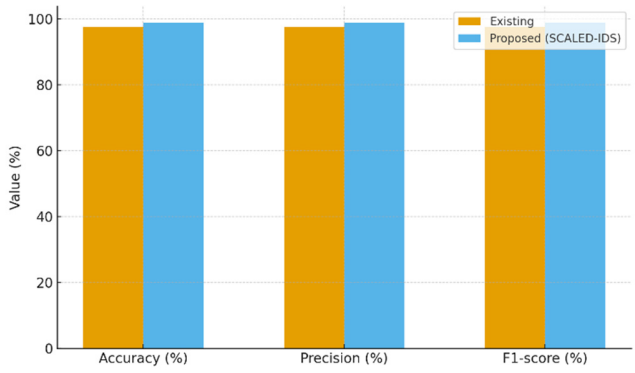

Fig. 3. Comparison with existing methods on CIC-IoT 2023.

Figure 4 presents the per-class F1-score comparison per individual attack category. The results reveal that SCALED-IDS not only maintains near-perfect detection for the majority classes, such as DDoS, DoS, and Mirai (F1-score~99.9%), but also significantly enhances performance on minority and challenging classes. In particular, the Web-Based and Brute Force attacks, which previously exhibited poor detection (F1-score 47.24% and 33.74% respectively), improved to 86.10% and 83.20%. Similarly, Reconnaissance and Spoofing attacks also benefited from an F1-score boost of over 10%.

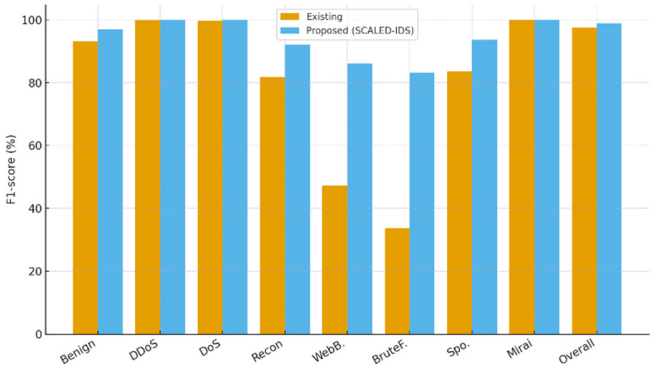

Fig. 4. Per-class F1-score results on the CIC-IoT 2023 dataset.

Table II presents the comparative performance analysis of the Existing System (ES) in [29] and the SCALED-IDS on the BoT-IoT dataset during the testing phase, highlighting the effectiveness and dominance of the latter across all key intrusion detection metrics and threat classes. Across all five threat classes, SCALED-IDS consistently outperforms the model in [29], showing improvements in accuracy, precision, recall, F1-score, and AUC. The DDoS class, for example, sees an improvement in precision from 98.48% to 98.90%, and F1-score from 96.30% to 96.95%, reflecting better detection of volumetric attacks. In the DoS class, the SCALED-IDS achieves a higher recall (97.45%) compared to ES (96.97%), which is critical for minimizing false negatives. For the Recon class, which often represents stealthy attacks, SCALED-IDS achieves near-perfect performance with 99.30% accuracy and 98.57% F1-score, outperforming the ES by a significant margin.

One of the most significant improvements is seen in the Theft class, which is a challenging category because of its limited sample size. Here, the SCALED-IDS boosts recall from 85.00% to 86.60% and F1-score from 89.47% to 90.60%, indicating better sensitivity to rare attack types. For the Normal (benign traffic) class, SCALED-IDS enhances classification performance by achieving 98.10% accuracy and a F1-score of 95.85%, reducing false positives and improving network trustworthiness. These improvements reflect the robust generalization ability of SCALED-IDS, along with its effectiveness in detecting both common and rare threats in IoT environments.

TABLE II. RESULTS ON BOT-IOT DATASET

Class	Metric	ES (TE) [29]	SCALED-IDS (TE)
DDoS	Accuracy	98.38%	98.75%
	Precision	98.48%	98.90%
	Recall	94.20%	95.10%
	F1-Score	96.30%	96.95%
	AUC	96.89%	97.35%
DoS	Accuracy	98.22%	98.65%
	Precision	96.39%	96.95%
	Recall	96.97%	97.45%
	F1-Score	96.68%	97.20%
	AUC	97.82%	98.25%
Recon	Accuracy	99.03%	99.30%
	Precision	97.72%	98.20%
	Recall	98.59%	98.95%
	F1-Score	98.07%	98.57%
	AUC	98.87%	99.10%
Theft	Accuracy	99.01%	99.20%
	Precision	94.44%	95.25%
	Recall	85.00%	86.60%
	F1-Score	89.47%	90.60%
	AUC	92.76%	93.40%
Normal	Accuracy	97.57%	98.10%
	Precision	93.63%	94.50%
	Recall	96.71%	97.30%
	F1-Score	95.15%	95.85%
	AUC	97.28%	97.60%
Average	Accuracy	98.51%	99.02%
	Precision	96.03%	96.85%
	Recall	94.29%	95.10%
	F1-Score	95.10%	95.92%
	AUC	96.66%	97.30%

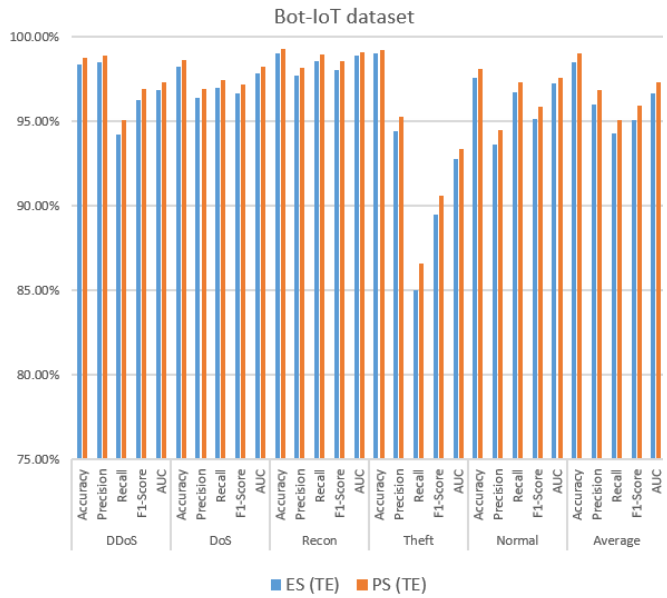

Fig. 5. Comparative evaluation of the system in [29] (ES) and SCALED-IDS (PS) on the BoT-IoT dataset.

A. *Comparison Analysis*

1) *CIC-IoT 2023 Dataset*

The proposed SCALED-IDS consistently outperforms the existing models on CIC-IoT 2023, with the overall Accuracy, Precision, and F1-score improving to 98.95%, 98.90%, and 98.92%, respectively. The proposed model achieves near-perfect detection for the majority classes of attacks, such as DDoS, DoS, and Mirai. Critically, minority classes, such as Web-Based and Brute Force, show huge F1-score gains, rising from 47.24% to 86.10% and 33.74% to 83.20%. These results highlight the robustness of SCALED-IDS in addressing class imbalance and enhancing intrusion detection reliability across diverse IoT attack categories.

2) *BoT-IoT Dataset*

This comparison demonstrates the consistent superiority of the SCALED-IDS across all metrics for each class and the overall average. The improvements are particularly prominent in the Theft class, which is traditionally challenging due to class imbalance. Here, SCALED-IDS significantly boosts Recall and F1-score, indicating enhanced sensitivity and fewer false negatives. For major attack categories, such as DDoS, DoS, and Recon, SCALED-IDS achieved nearly perfect precision and F1-scores, indicating highly accurate classification with minimal misclassification. Even in the Normal class, which is vital for avoiding false alarms, SCALED-IDS maintains a noticeable lead in all metrics. The average performance across all classes is higher, reinforcing its overall robustness, precision, and generalization capability. This performance advantage is likely attributed to the advanced architectural components of SCALED-IDS, such as threat-aware learning CAFEs and divide-and-conquer decoding, enabling it to effectively adapt to complex and imbalanced IoT network data.

V. CONCLUSION

This paper presented SCALED-IDS, a deep learning-based intrusion detection framework designed to address the challenges of multiclass attack detection in cloud-integrated IoT environments. The model introduces a modular architecture composed of MARE, CAFEs, and CLAD. Together, these components enable the system to capture semantic dependencies in traffic data, enhance class-specific discrimination, and improve hierarchical classification across diverse attack categories. Through extensive experiments on the BoT-IoT and CIC-IoT 2023 datasets, SCALED-IDS demonstrated superior performance in detecting both dominant and minority attacks. The results confirm the framework's ability to overcome limitations present in traditional and existing deep learning-based IDS methods—particularly in handling class imbalance, ensuring interpretability, and achieving scalability in high-volume cloud-IoT settings. Given its robustness and effectiveness, SCALED-IDS presents itself as a promising solution to improve real-time network security in future smart environments. As part of future work, the model can be extended to support adaptive online learning, transferability across unseen domains, and real-world deployment using collaborative edge-cloud architectures. Additionally, investigating its resilience in adversarial settings and resource-constrained conditions will further strengthen its applicability in next-generation IoT security frameworks.

REFERENCES

[1] H. Sadia *et al.*, "Intrusion Detection System for Wireless Sensor Networks: A Machine Learning Based Approach," *IEEE Access*, vol. 12,

pp. 52565–52582, 2024, https://doi.org/10.1109/ACCESS.2024.3380014.

[2] A. Binbusayyis, "Innovative Defense: Deep Learning-Powered Intrusion Detection for IoT Networks," *IEEE Access*, vol. 13, pp. 31105–31120, 2025, https://doi.org/10.1109/ACCESS.2025.3542275.

[3] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019, https://doi.org/10.1109/ACCESS.2019.2907965.

[4] V. Gaur and R. Kumar, "Analysis of Machine Learning Classifiers for Early Detection of DDoS Attacks on IoT Devices," *Arabian Journal for Science and Engineering*, vol. 47, no. 2, pp. 1353–1374, Feb. 2022, https://doi.org/10.1007/s13369-021-05947-3.

[5] Kamaldeep, M. Malik, and M. Dutta, "Feature Engineering and Machine Learning Framework for DDoS Attack Detection in the Standardized Internet of Things," *IEEE Internet of Things Journal*, vol. 10, no. 10, pp. 8658–8669, Feb. 2023, https://doi.org/10.1109/JIOT.2023.3245153.

[6] Ismail *et al.*, "A Machine Learning-Based Classification and Prediction Technique for DDoS Attacks," *IEEE Access*, vol. 10, pp. 21443–21454, 2022, https://doi.org/10.1109/ACCESS.2022.3152577.

[7] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Applied Sciences*, vol. 13, no. 17, Jan. 2023, Art. no. 9937, https://doi.org/10.3390/app13179937.

[8] W. Sheng and J. Zhigang, "IDS classification algorithm based on fuzzy SVM models," *Application Research of Computers*, vol. 37, no. 2, 2018.

[9] J. Gu and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," *Computers & Security*, vol. 103, Apr. 2021, Art. no. 102158, https://doi.org/10.1016/j.cose.2020.102158.

[10] B. Mahbooba, M. Timilsina, R. Sahal, and M. Serrano, "Explainable Artificial Intelligence (XAI) to Enhance Trust Management in Intrusion Detection Systems Using Decision Tree Model," *Complexity*, vol. 2021, no. 1, 2021, Art. no. 6634811, https://doi.org/10.1155/2021/6634811.

[11] W. W. Lo, S. Layeghy, M. Sarhan, M. Gallagher, and M. Portmann, "E-GraphSAGE: A Graph Neural Network based Intrusion Detection System for IoT," in *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*, Budapest, Hungary, Apr. 2022, pp. 1–9, https://doi.org/10.1109/NOMS54207.2022.9789878.

[12] L. Chang and P. Branco, "Graph-based Solutions with Residuals for Intrusion Detection: the Modified E-GraphSAGE and E-ResGAT Algorithms." arXiv, Nov. 26, 2021, https://doi.org/10.48550/arXiv.2111.13597.

[13] X. Deng, J. Zhu, X. Pei, L. Zhang, Z. Ling, and K. Xue, "Flow Topology-Based Graph Convolutional Network for Intrusion Detection in Label-Limited IoT Networks," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 684–696, Mar. 2023, https://doi.org/10.1109/TNSM.2022.3213807.

[14] G. Duan, H. Lv, H. Wang, and G. Feng, "Application of a Dynamic Line Graph Neural Network for Intrusion Detection With Semisupervised Learning," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 699–714, 2023, https://doi.org/10.1109/TIFS.2022.3228493.

[15] X. Hu, W. Gao, G. Cheng, R. Li, Y. Zhou, and H. Wu, "Toward Early and Accurate Network Intrusion Detection Using Graph Embedding," *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 5817–5831, 2023, https://doi.org/10.1109/TIFS.2023.3318960.

[16] H. Nguyen and R. Kashef, "TS-IDS: Traffic-aware self-supervised learning for IoT Network Intrusion Detection," *Knowledge-Based Systems*, vol. 279, Nov. 2023, Art. no. 110966, https://doi.org/10.1016/j.knosys.2023.110966.

[17] S. Huan *et al.*, "T-Shaped CAN Feature Integration With Lightweight Deep Learning Model for In-Vehicle Network Intrusion Detection," *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 12, pp. 21183–21196, Dec. 2024, https://doi.org/10.1109/TITS.2024.3478371.

[18] F. S. Alrayes, N. Nemri, N. Aljaffan, A. Alshuhail, A. A. Alhashmi, and A. Mahmud, "Distributed Multiclass Cyberattack Detection Using Golden Jackal Optimization With Deep Learning Model for Securing IoT Networks," *IEEE Access*, vol. 12, pp. 132434–132443, 2024, https://doi.org/10.1109/ACCESS.2024.3443202.

[19] U. C. Akuthota and L. Bhargava, "Transformer-Based Intrusion Detection for IoT Networks," *IEEE Internet of Things Journal*, vol. 12, no. 5, pp. 6062–6067, Mar. 2025, https://doi.org/10.1109/JIOT.2025.3525494.

[20] M. Huang, Y. Lin, N. Li, X. Chen, and E. Bertino, "CARD: Robustness-Preserving Transfer Learning for Network Intrusion Detection via Contrastive Adversarial Representation Distillation," *IEEE Transactions on Dependable and Secure Computing*, vol. 22, no. 5, pp. 5134–5151, Sep. 2025, https://doi.org/10.1109/TDSC.2025.3562600.

[21] N. Koroniotis, N. Moustafa, E. Sitnikova, and J. Slay, "Towards Developing Network Forensic Mechanism for Botnet Activities in the IoT Based on Machine Learning Techniques," in *Mobile Networks and Management*, vol. 235, J. Hu, I. Khalil, Z. Tari, and S. Wen, Eds. Springer International Publishing, 2018, pp. 30–44.

[22] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, Sep. 2020, https://doi.org/10.1016/j.future.2020.03.042.

[23] N. Koroniotis and N. Moustafa, "Enhancing network forensics with particle swarm and deep learning: The particle deep framework." arXiv, May 02, 2020, https://doi.org/10.48550/arXiv.2005.00722.

[24] N. Koroniotis, N. Moustafa, F. Schiliro, P. Gauravaram, and H. Janicke, "A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports," *IEEE Access*, vol. 8, pp. 209802–209834, 2020, https://doi.org/10.1109/ACCESS.2020.3036728.

[25] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "CICIoT2023: A Real-Time Dataset and Benchmark for Large-Scale Attacks in IoT Environment," *Sensors*, vol. 23, no. 13, Jan. 2023, Art. no. 5941, https://doi.org/10.3390/s23135941.

[26] V. Borisov, J. Haug, and G. Kasneci, "CancelOut: A Layer for Feature Selection in Deep Neural Networks," in *Artificial Neural Networks and Machine Learning – ICANN 2019: Deep Learning*, 2019, pp. 72–83, https://doi.org/10.1007/978-3-030-30484-3_6.

[27] A. Ghorbani and S. M. Fakhrahmad, "A Deep Learning Approach to Network Intrusion Detection Using a Proposed Supervised Sparse Auto-encoder and SVM," *Iranian Journal of Science and Technology, Transactions of Electrical Engineering*, vol. 46, no. 3, pp. 829–846, Sep. 2022, https://doi.org/10.1007/s40998-022-00498-1.

[28] I. A. Nellas, S. K. Tasoulis, V. P. Plagianakos, and S. V. Georgakopoulos, "Supervised Dimensionality Reduction and Image Classification Utilizing Convolutional Autoencoders." arXiv, Nov. 03, 2022, https://doi.org/10.48550/arXiv.2208.12152.

[29] D. Bian and J. Liu, "GMCWAE: A Representation Learning Technique for Network Intrusion Detection in IoT," *IEEE Internet of Things Journal*, vol. 12, no. 12, pp. 20343–20356, Jun. 2025, https://doi.org/10.1109/JIOT.2025.3542845.