THE ASIAN BULLETIN OF BIG DATA MANAGMENT
Vol. 6. Issue 1 (2026)
https://doi.org/10.62019/n87ayj75

Internet Of Things Intrusion Detection Based on Deep Learning

Fauzia Talpur, Mir Rahib Hussain Talpur*, Adeel Kamran, Shakir Hussain Talpur, Syed Baig Ali Shah, Khan Muhammad Maher

Chronicle

Article history
Received: Nov24 12, 2025
Received in the **revised format:** Dec18, 2025
Accepted: Jan 5, 2026
Available online: Jan 26 2026

Fauzia Talpur is currently affiliated with Information Technology Centre, Sindh Agriculture University Tandojam.

Email: fozia.g.talpur@gmail.com

Mir Rahib Hussain Talpur*, Adeel Kamran, Shakir Hussain Talpur, Syed Baig Ali Shah, & Khan Muhammad Maher, are currently affiliated with the Institute of Information Technology Centre, Sindh Agriculture University Tandojam, Pakistan.

Email: rahibtalpur@gmail.com

Corresponding Author

Abstract

The fast-growing Internet of Things (IoT) has exposed more attack vectors of the connected devices and heightened the necessity of effective intrusion detection systems (IDS). Nevertheless, the three main challenges that still limit the practical use of IoT intrusion detection include the high complexity of models that are only runnable on resource-constrained devices, low generalization in the presence of small and unbalanced labelling, and the lack of privacy-concerning collaborative detection systems among heterogeneous settings. Here, it is possible to identify a multi-stage research program based on three complementary frameworks that consolidate these challenges in this paper. The main shortcoming of the paper is that the authors first propose lightweight intrusion detection model, LIIDXC, to describe binary XNOR-based convolution of a two-layer long short-term memory (LSTM) and entropy-guided feature selection with a focus on computational overhead reduction without losing detection power. Second, a superior framework of transfer learning, EMTD-SSC, combines a residual convolutional autoencoder, multilayer multi-kernel maximum mean discrepancy (MLMK-MMD) along with fine-tuning techniques to enhance cross-domain transfer when the sample size is small. Third, a federated contrastive learning framework, ID-CFL, enables collaborative intrusion detection without raw data sharing and improves robustness under non-IID client distributions by adaptive node-correlation aggregation. Experiments on N-BaIoT, CIC-DDoS2019, IoT-23, ToN-IoT, and BoT-IoT demonstrate that LIIDXC achieves 87.4% accuracy with approximately fivefold training acceleration, EMTD-SSC reaches up to 94.8% accuracy and maintains 82.8% accuracy with only 100 samples per class, and ID-CFL attains 84.79% average personalized local-client accuracy while improving non-IID collaborative detection performance by up to 38% relative to conventional federated baselines. Taken together, the results show that lightweight computation, cross-domain knowledge transfer, and privacy-preserving distributed learning can be integrated into a coherent IoT IDS research agenda that is efficient, robust, and scalable.

Keywords: Internet of Things, intrusion detection system, XNOR-CNN, binary neural networks, transfer learning, federated learning, contrastive learning, deep learning, cybersecurity

INTRODUCTION

The Internet of Things (IoT) has transformed communication infrastructures by connecting large numbers of smart, embedded, and often resource-constrained devices across homes, healthcare, transportation, manufacturing, and critical infrastructure. As device density and service dependence increase, IoT networks have become attractive targets for malware propagation, botnet recruitment, remote exploitation, denial-of-service activity, and privacy compromise. Conventional perimeter defenses such as firewalls and antivirus tools are not sufficient for this setting because they are generally static, signature-dependent, or blind to dynamic traffic

behavior. Intrusion detection systems (IDS) remain essential because they provide continuous traffic monitoring and can identify deviations from normal or expected communication patterns. IoT intrusion detection differs from traditional network intrusion detection in at least three respects. First, the protected endpoints are usually constrained in memory, storage, and computation. Second, IoT traffic is heterogeneous in protocol structure, behavior, and device role. Third, attack patterns evolve quickly, making concept drift and class imbalance particularly difficult for supervised models. These characteristics create a need for intrusion detection mechanisms that are accurate, lightweight, adaptive, and deployable across distributed environments.

Table 1.

Comparative characteristics of IoT intrusion detection and traditional network intrusion detection.

Category	IoT Intrusion Detection	Traditional Network Intrusion Detection
Primary Objective	Protect IoT devices connected to the internet (low computational power, limited storage)	Protect entire network infrastructures, including servers.
Architecture	Distributed architecture (reduces burden on central servers, improves response time)	Centralized architecture (easier management and monitoring)
Challenges	Concept drift (IoT attacks evolve-dynamically) High Dimensional data processing Computing efficiency	Handling large volumes of attack traffic Data imbalance Model interpretability

However, even with the advancement of deep learning on the sphere of cybersecurity, three unclear barriers restrain the practical implementation of the use of an IoT IDS. The former is the redundancy of computation: many deep model versions continue to be too complex to run on edge-class computing engine. The second one is data sparseness and domain shift: the labeled intrusion data can be very small, unbalanced, or irrelevant to the target operating environment, and this reduces generalization. The third one is the absence of collaborative privacy-aware learning: the IoT devices are in a distributed and fragmented location and administratively, however, the training is centralized, which makes privacy, communication, and scalability issues.

Earlier studies have typically conceived these problems in a vacuum. Lightweight IDS studies tend to make efficiency rather than accuracy tradeoffs. Transfer learning research is known to increase adaptation, but it often uses more labeled data than would be available in new applications. Protecting privacy Federated learning studies, however, have poor uniqueness-independence (IID) behaviour under highly non-IID label distributions and traffic distributions commonly observed in the IoT. ***Integrated research*** has thus been required to research resource efficiency, data-efficient adaptation and collaborative privacy-preserving detection as mutually correlated issues and not design independent issues.This paper has four connected goals: (i) to create a lightweight deep learning model that retains the same detection performance with limited computation; (ii) to create a transfer learning system that is effective when labeled target-domain data is limited; (iii) to create a collaborative federated intrusion detection system that does not require sharing of raw data, but has the same vulnerability to heterogeneous client distributions; and (iv) to test these designs with several public intrusion datasets with similar experimental metrics.

Main Contributions

There are three key contributions that this thesis summarized in this paper contains. The first is the lightweight IDS, LIIDXC, that combines XNOR-based binary convolution with temporal modeling with the help of a two-layer LSTM and entropy-based feature selection. Second, it suggests EMTD-SSC, a framework of transfer learning, which is constructed on a residual convolutional autoencoder and multilayer multi-kernel maximum mean discrepancy to assist cross-domain detection in the event of significantly few samples. Third, it suggests the ID-CFL, a federated contrastive learning system that does nodecorrelation aggregation to collaboratively detect intrusion among heterogeneous clients of the IoT inference system. These contributions taken collectively answer the question of computation, data availability, and privacy-preserving collaboration in a single coherent IoT IDS research program.

Related Work

Intrusion detection has developed into the rudimentary host-based monitoring and the specialist system to more network-based anomaly detection and, more lately, security analytics driven by data. Within the framework of the IoT, the anomaly detection strategies can be categorized into statistical, classical machine learning, and deep learning techniques.

Statistical processes are used to model normal traffic based on distributional assumptions, thresholding or dimensionality reduction. They are conceptually straightforward and can be useful to well-characterized environments, but are frequently afflicted with large false-alarm rates in dynamic IoT traffic and can be poorly used to characterize more sophisticated attacks. Classical machine learning approaches, including decision trees, support vector machines, K-nearest neighbors, and hidden Markov models, are more effective at improving discriminative performance, but often need handcrafted features, and often have to be redesigned with network behavior responses.

Deep learning approaches have been successful since they acquire hierarchical representations of traffic only through raw or lightly processed intensities. Applications of CNNs are useful in the local spatial features extraction, temporal dynamics, including LSTM, and the unsupervised or weakly supervised detection of anomalies. Rare classes or systems, learn latent attacks structure, or learn dependencies in the model system have also been augmented with GANs, deep belief networks, or graph-based models.

There are three recent work trends that would be most applicable to this research. The former is about models that are lightweight and deep models, in particular model compression, quantization, and binary neural networks which simplify arithmetic and memory use. The second is related to transfer learning and domain adaptation and residual structures, feature alignment losses, and fine-tuning methods prevent the problem of mismatched domain. The third is about federated learning, where distributed clients have the opportunity to learn common models without local data disclosure, although facilitation in client distributions still has some efficacy.

There is however a gap left in the literature. Lightweight models are seldom combined with sequential attack modeling; transfer learning algorithms are seldom tested with very small sample per-class constraints; federated IoT IDS models typically make use of conventional aggregation algorithms like a FedAvg, which do not resist client drift in non-IID settings. The current work fills this gap by creating three frameworks, which are not competing but complementary, namely lightweight local inference, cross-domain adaptation, and collaborative privacy-preserving detection.

MATERIALS AND METHODS

Overall Research Design

The entire research design will follow the format of a series of individual-device and cross-domain adaptation and eventually collaborative distributed learning. Framework 1 addresses constrained deployment in the case of resources using a lightweight deep intrusion detection task. Framework 2 involves limited supervision of the target domain through the transfer of knowledge of a source domain to a target IoT domain. Framework 3 allows expanding intrusion detection to clients by using privacy-preserving federated learning. Despite being experimentally different, these frameworks address the same design principle: IoT IDS is supposed to be accurate within the limitation at the operation of the system rather than in an idealized centralized environment.

Proposed Framework 1: LIIDXC Lightweight XNOR-CNN-LSTM Model

The LIIDXC architecture is fed preprocessed the records of benign and malicious traffic on a network, transforms them into formats acceptable by the two-dimensional convolutional features of binary convolutional feature extraction, and temporal refines them using two-layer LSTM refinements. In the last step, the resultant probabilities of the classes are obtained via a Softmax classifier. In order to make the convolutional layers simpler, the activations and the weights are binarized and allow multiplication-free XNOR operations. The principle component analysis is also used with information entropy to enhance feature selection by ensuring that the selected inputs retain discriminative variation, but reduce important dimensions.

The design of the architecture was aimed at maintaining the strong points of hybrid CNN-LSTM intrusion detectors at the expense of lessening the overall computational load of the designs otherwise making it inaccessible to edge-class devices. The convolutional part has the advantage of capturing the structural traffic patterns but the LSTM part helps in the temporal reliance measures in packets or flow series. The translatorically compiled binary version swaps costly floating point multiplications with bit logic, thus trimming down the model as well as pace training and inference.

Proposed Framework 2: EMTD-SSC Transfer Learning Model

The second structure pertains to the issue of the small sample of preliminary detection of intrusion in IoT through a combination of transfer learning, feature matching, and residual representation learning. The model works with five modules, as data is collected, preprocessed, pre-trained on the source domain, and transferred to the target domain, and the ultimate intrusion detection is improved. A key characteristic of it is its core feature extractor that is represented by a dual residual convolutional autoencoder (RCAE), that trains efficient latent representations and removes information loss in later-layers networks using skip connections.

The transfer stage aligns the distributions of features between the source and target domain on the basis of multilayer multikernel maximum mean discrepancy. In its design, this technology enables the utilization of knowledge based on a larger or more mature intrusion dataset to enhance performance in a target IoT environment where the availability of labeled data are limited. Training a bottleneck classifier is supervised on labeled source-domain data, so a minimization of reconstruction error is minimized by the autoencoder at the same time, ultra- increasing a representation that will be transferable and discriminative. It is thus a representation learning framework template that incorporates domain adaptation, and selective fine-tuning in one an optimization pipeline.

Proposed Framework 3: ID-CFL Federated Contrastive Learning Model

This research aims to back the proposed study framework that seeks to develop a Federated Contrastive Learning Model grounded in ID-CFL.The third framework expands the scope of the IoT intrusion detection not only in local or cross-domain, but in a distributed collaborative setting. ID-CFL is hierarchized into a device layer, a local client layer and a cloud central service layer. The heterogeneous traffic of the IoT is collected and processed by the device layer. Local deep models are trained to use local contrastive representation learning and classification as the objective on the local client layer. The cloud layer combines updates of clients and reallocates the enhanced global model without the clients sending raw traffic data.

The primary issue with federated IoT learning is the non-IID distribution of traffic and labels among clients. The model may be adversely affected by local biased updates in standard averaging, as well as be overemphasized. ID-CFL thus uses node-correlation aggregation where covariance by skewness-based statistics visualize the statistical variations in the contribution of a client at global aggregation time. Also contrastive learning is applied to minimize reliance on explicit labeling by encouraging similar examples to cluster together in representation space and dissimilar or anomalous examples to be separated.

Mathematical Formulations

This section retains the core mathematical structure of the three frameworks while presenting it in condensed journal form.

Binary Convolution in LIIDXC

For an input feature map F of size w × h × C and a convolution kernel K of size k × k × C, the standard convolution at location (i, j) for filter n is written as follows.

$$O_{i,j,n} = \Sigma_{c=1}^{C} \Sigma_{p=1}^{k} \Sigma_{q=1}^{k} F_{i+p-1,j+q-1,c} \cdot K_{p,q,c,n} \quad (1)$$

In the binary convolutional network, the weight tensor is approximated by a binary filter B and a positive scaling factor a, such that $W \approx aB$ with $B \in \{+1, -1\}^{c,w,h}$. The convolution can then be estimated through XNOR-based operations.

$$I * W \approx a (I \otimes B) \quad (2)$$

$$O_{i,j,n} = \Sigma_{c=1}^{C} \Sigma_{p=1}^{k} \Sigma_{q=1}^{k} (F_{i+p-1,j+q-1,c} \otimes W_{p,q,c,n}) \times 2 - 1 \quad (3)$$

This replacement reduces the need for floating-point multiplication and substantially decreases memory use because binary filters require one bit per parameter instead of conventional high-precision storage.

Transfer Learning Loss in EMTD-SSC

Let x^S and x^T denote source- and target-domain samples, respectively. The MK-MMD term measures discrepancy between source and target feature distributions in a reproducing kernel Hilbert space. The optimized multilayer form used in EMTD-SSC is expressed as:

$$L_{MK\text{-}MMD}(x^S,x^T) = \| (1/n_S) \Sigma_{i=1}^{n_S} G_S(x_i^S) - (1/n_T) \Sigma_{i=1}^{n_T} G_T(x_i^T) \|_{H_K}^2 \quad (4)$$

$$L_{MLMK\text{-}MMD} = \Sigma_{k=1}^{K} MK\text{-}MMD(G_S^k(x^S), G_T^k(x^T)) \quad (5)$$

The residual convolutional autoencoder further minimizes reconstruction loss, while labeled source-domain samples drive supervised classification in the bottleneck layer.

$$L_{RE} = (1/n_S) \Sigma_{i=1}^{n_S} l(x_i^S, \hat{x}_i^S) + (1/n_T) \Sigma_{i=1}^{n_T} l(x_i^T, \hat{x}_i^T) \quad (6)$$

$$L_{SE} = \Sigma_{i=1}^{n_S} \Sigma_{j=1}^{m} y_{i,j}^S \log z_{i,j}^S \quad (7)$$

$$L_{EMTD\text{-}SSC} = L_{MLMK\text{-}MMD} + L_{RE} + L_{SE} \quad (8)$$

Federated Objective and Contrastive Similarity in ID-CFL

For a distributed dataset D = {(x_i, y_i)}, local clients optimize a task loss over their own samples while contributing updates to a global model parameterized by θ.

$$L(\theta) = (1/n) \Sigma_{i=1}^{n} L(y_i, f_\theta(x_i)) \quad (9)$$

The contrastive component uses kernel-based similarity to encourage favorable geometry in representation space.

$$K(x_i,x_j) = \exp(- \|x_i - x_j\|^2 / 2\sigma^2) \quad (10)$$

$$L_{con} = (1/|D|) \Sigma_{D} [y_i y_j K(x_i,x_j) + (1 - y_i y_j) 1/2 (K(x_i,x_j)^2 - K(x_i,x_i) - K(x_j,x_j))] \quad (11)$$

After local optimization, the server updates the global model by aggregating client gradients or weights through an adaptive rule. In condensed form, the global update can be expressed as:

$$\omega^{t+1} = \omega^t + \beta ((1/K) \Sigma_{k=1}^{K} \nabla\omega_k^{t+1} - \omega^t) \quad (12)$$

In ID-CFL, the effective contribution of each client is further adjusted using covariance- and skewness-derived node-correlation statistics, which reduces the effect of biased or weakly aligned local updates.

Algorithms and Model Training Procedure

The LIIDXC training process binarizes both input tensors and filter weights, performs forward propagation through XNOR-based convolution, computes the classification loss, and updates real-valued latent weights through gradient-based optimization while preserving a binary forward path. The EMTD-SSC training procedure alternates between source-domain supervised learning, autoencoder reconstruction, and source-target alignment using MLMK-MMD, followed by controlled fine-tuning of selected layers. The ID-CFL procedure initializes a global model, distributes it to selected clients, performs local contrastive and classification training, computes node-correlation statistics, and then aggregates local updates into a new global model before the next communication round.

Across the three frameworks, the training strategy reflects the intended deployment context. LIIDXC prioritizes computational economy; EMTD-SSC prioritizes transferability under scarce supervision; and ID-CFL prioritizes distributed robustness and privacy preservation.

EXPERIMENTAL SETUP

Datasets

The experimenta campaign uses several public benchmark datasets selected to match the design goals of the three frameworks. LIIDXC is primarily evaluated on the N-BaIoT dataset, which contains benign and attack traffic collected from heterogeneous consumer IoT devices. EMTD-SSC is evaluated using CIC-DDoS2019 and IoT-23 to study cross-domain transfer from a richer source domain to a smaller or behaviorally different target domain. ID-CFL is evaluated on ToN-IoT and BoT-IoT to assess collaborative detection across distributed clients.

Table 2.
N-BaIoT traffic distribution used for LIIDXC experiments.

Dataset ID	Device Name	Benign Traffic	Attack Traffic
IoT-1	Danmini-Doorbell	49548	968750
IoT-2	Ecobee-Thermostat	13113	822763
IoT-3	Ennio-Doorbell	39100	316400
IoT-4	Philips B120N/10-Baby Monitor	175240	923437
IoT-5	Provision PT-737E-Security Camera	62154	766106
IoT-6	Provision PT-838-Security Camera	98514	738377
IoT-7	Samsung SNH 1011 N-Webcam	52150	323072
IoT-8	SimpleHome XCS7-1002-WHT-Security Camera	46585	816471
IoT-9	SimpleHome XCS7-1003-WHT-Security Camera	19528	831298

Preprocessing

Preprocessing varied by framework but followed a common sequence of data reading and labeling, data cleaning, standardization of record length, categorical encoding, normalization, and train-test partitioning. For LIIDXC, preprocessing also included balancing through under-sampling and entropy-guided feature selection before reshaping records for two-dimensional convolution. For EMTD-SSC, preprocessing further involved identification of highly correlated features and feature importance ranking to support stable cross-domain representation learning. For ID-CFL, traffic was grouped into packet sequences or flow windows suitable for local contrastive modeling.

Evaluation Metrics

Performance was evaluated with accuracy, precision, recall, macro-F1 score, and false positive rate where appropriate. For federated settings, personalized local-client accuracy and communication efficiency across rounds were also examined. These

metrics were selected to avoid overreliance on accuracy alone, especially under class imbalance.

Hyperparameters and Training Settings

The original thesis reports framework-specific training settings, including dataset partition ratios, numbers of training iterations, learning configurations, fine-tuning depth, kernel widths, and client selection ratios. In LIIDXC, time-efficiency experiments were conducted using 50%, 80%, and 100% of the training data for 100 iterations. In EMTD-SSC, ablations examined the number of fine-tuned layers, the depth of the residual convolutional autoencoder, and kernel widths from 16 to 512. In ID-CFL, client selection ratios and communication rounds were varied to evaluate convergence, personalization, and robustness under non-IID label distributions.

RESULTS

Results for LIIDXC

LIIDXC outperformed the compared baseline models in binary intrusion detection on N-BaIoT. The model achieved 87.4% accuracy, 87.2% precision, 87.6% recall, and 87.4% macro-F1, surpassing conventional machine learning baselines and stronger deep baselines such as CNN-LSTM and DCAE. These gains indicate that binary convolution, when combined with temporal modeling, can preserve discriminative capacity rather than merely compressing the model.

The fine-grained analysis reported in the thesis also showed that LIIDXC achieved the best precision and recall for benign, Bashlite, and Mirai traffic categories, suggesting that the hybrid spatial-temporal binary design preserves class-sensitive patterns even under aggressive quantization.

Table 3.
Binary-classification performance of LIIDXC against baseline models.

Model	Accuracy (Acc)	Precision (P)	Recall (R)	Macro F1 (M-F1)
KNN	84.3%	84.5%	84.7%	84.6%
MLP	83.7%	83.6%	83.8%	83.7%
ID3	83.8%	83.3%	83.9%	83.6%
BotCatcher	83.6%	83.4%	83.7%	83.5%
2D-CNN	84.5%	84.2%	84.4%	84.3%
LSTM	83.1%	83.2%	83.3%	83.2%
DCAE	85.5%	85.2%	85.3%	85.2%
CNN-LSTM	86.1%	86.5%	86.6%	86.6%
LIIDXC	87.4%	87.2%	87.6%	87.4%

Time-efficiency analysis further demonstrated the practical value of binarization. Training time increased only modestly as the training set expanded from 50% to 100%, which supports the claim that LIIDXC is less sensitive to data scale than standard floating-point models.

Table 4.
LIIDXC average training time under different data proportions.

Data Proportion	Time (Seconds)
50%	31.42
80%	37.84
100%	40.56

RESULTS FOR EMTD-SSC

EMTD-SSC yielded strong cross-domain performance and remained effective under severe label scarcity. Ablation results showed that deeper fine-tuning substantially improved performance: tuning more than three layers raised accuracy to 92.3% and macro-F1 to 92.1, compared with 81.2% accuracy without fine-tuning. This indicates that partial adaptation is insufficient when source and target IoT domains diverge meaningfully in traffic behavior.

Table 5.
Effect of fine-tuning depth on EMTD-SSC performance.

Fine Tuning Strategy	Accuracy (ACC)	Precision (P)	Recall (R)	Macro F1-Score (M-F1)
No Fine Turning	81.2	80.6	81.3	80.9
Fine Tuning One Layers	81.5	80.7	81.5	81.1
Fine Tuning Two Layers	82.3	82.1	82.6	82.3
Fine Tuning Three Layers	85.6	85.4	86.8	86.1
Fine Tuning more than three layers	92.3	91.7	92.5	92.1

Kernel-width analysis showed that a width of 128 gave the best mean performance (91.3 ± 0.16), with 256 performing nearly as well. Very narrow kernels under-captured features, whereas excessively wide kernels did not provide further benefit and in some cases degraded performance slightly.

Table 6.
Sensitivity of EMTD-SSC to convolutional kernel width.

Kernel Width	Accuracy
16	84.4 ± 0.13
32	89.5 ± 0.13
64	90.2 ± 0.14
128	91.3 ± 0.16
256	91.1 ± 0.12
512	90.1 ± 0.15

The strongest evidence of the method's utility appears in the small-sample experiments. With only 100 samples per class, EMTD-SSC reached 82.8% accuracy, whereas GPIoT and MENSA remained near 53%-55%. As the number of samples increased, EMTD-SSC continued to lead and remained above 92% once the training budget reached 2000 samples per class.

Table 7.
Accuracy under varying target-domain sample sizes

Samples per Class	GPIoT Accuracy	MENSA Accuracy	EMTD-SSC Accuracy
100	53.2	54.7	82.8
500	57.4	58.3	89.3
1000	63.3	64.8	91.9
2000	69.1	77.1	92.3
3000	71.8	85.3	92.6
4000	72.3	86.7	92.9
5000	72.3	86.7	92.3

.In cross-domain binary classification across ten scenarios, EMTD-SSC achieved the highest average accuracy among all compared models. Averaged over the reported scenarios, EMTD-SSC reached approximately 92.33%, exceeding DeepTraLog (85.81%), FTL (85.62%), MENSA (84.11%), and P-ResNet (83.08%). In the fine-grained comparison, EMTD-SSC also achieved the strongest precision, recall, and macro-F1, while reducing the false positive rate to 0.35.

Table 8.
Fine-grained comparison of EMTD-SSC with representative transfer learning and deep learning baselines.

Model	Precision (P)	Recall (R)	Macro F1 (M-F1)	False Positive Rate (FPR)
P-ResNet	83.3	81.2	82.2	1.26
HetIoT	76.5	75.8	76.1	1.33
GPIoT	73.4	72.5	72.9	1.35
FTL	77.5	76.9	77.2	1.28
JSTN	86.7	86.5	86.6	1.14
MENSA	86.1	85.3	85.7	1.18
DeepAID	80.6	81.1	80.8	1.22
DeepPTragLog	85.4	84.9	85.1	1.17
EMTD-SSC	92.7	92.2	92.4	0.35

Results for ID-CFL

The federated experiments show that ID-CFL substantially improves collaborative intrusion detection under heterogeneous client distributions. On the personalized local-client evaluation, ID-CFL achieved an average accuracy of 84.79%, compared with 54.46 for FedAvg, 65.91 for FedProx, 81.79 for Scaffold, and 75.65 for FedAGM. The gain over FedAvg was especially large on difficult clients, confirming that node-correlation aggregation mitigates client drift under non-IID distributions.

Table 9.

Client	FedAvg	FedProx	Scaffold	FedAGM	ID-CFL
1	65.13	73.26	78.78	79.43	82.93

Client	FedAvg	FedProx	Scaffold	FedAGM	ID-CFL
2	55.28	62.37	82.16	78.65	86.66
3	47.65	64.52	83.33	75.34	84.35
4	44.37	60.68	79.98	73.45	85.27
5	52.63	61.36	80.13	75.66	81.65
6	47.03	70.25	81.27	71.28	86.59
7	50.26	69.87	82.43	75.48	83.04
8	57.85	66.43	83.86	77.73	86.27
9	60.12	61.77	81.88	74.26	85.48
10	64.32	68.54	84.23	75.23	85.62
Avg	54.46	65.91	81.79	75.65	84.79

Personalized local-client accuracy comparison for federated learning methods.

The thesis also reports collaborative detection gains on both ToN-IoT and BoT-IoT. Averaged across the listed scenarios, ID-CFL achieved 87.71% on ToN-IoT and 86.33% on BoT-IoT, clearly outperforming FedAvg, FedProx, Scaffold, FedAGM, MENSA, and DeepTraLog. In extreme label-bias settings, the model reportedly improved performance by as much as 38% over FedAvg. Communication-efficiency analysis further showed that ID-CFL converged after roughly 50 communication rounds and achieved lower loss than the competing federated baselines under equal iteration budgets.

Table 10.
Average cross-domain binary-classification accuracy across the ten reported scenarios

Model	Average Accuracy Across 10 Cross-Domain Scenarios
P-ResNet	83.08
HetIoT	76.15
GPIoT	74.27
DeepAID	76.33
DeepTraLog	85.81
FTL	85.62
JSTN	79.72
MENSA	84.11
EMTD-SSC	92.33

Table 11. Average collaborative detection accuracy by dataset for federated baselines and ID-CFL.

Dataset	FedAvg	FedProx	Scaffold	FedAGM	MENSA	DeepTraLog	ID-CFL
BoT-IoT	68.54	71.44	72.13	73.34	64.20	64.17	86.33
ToN_IoT	68.05	71.02	72.08	73.61	65.69	65.14	87.71

DISCUSSION

Significance of Findings

The results show that the three frameworks are complementary solutions to different operational bottlenecks in IoT security. LIIDXC demonstrates that binary convolution can be used for practical IDS deployment without collapsing accuracy, provided that temporal dependencies are modeled through LSTM and features are selected carefully. EMTD-SSC demonstrates that cross-domain alignment and residual representation learning can make transfer learning effective even when the target domain contains very few labeled samples. ID-CFL demonstrates that privacy-preserving collaborative training need not rely on naive averaging; adaptive aggregation materially improves learning under heterogeneous client behavior.

comparison with Previous Methods

selative to the traditional machine learning baselines, LIIDXC performed superiorly in detection whilst minimizing the computational cost. Compared to the latest transfer-learning and deep-learning baselines, EMTD-SSC had the highest cross-domain and the largest difference when training sample sizes were exceptionally small. In comparison with conventional federated baselines, ID-CFL repeatedly enhanced personalized and collaborative accuracy which is especially significant since the deployment of IoTs is not usually IID in practice.

Strengths

The primary strength of this work is the breadth of the methods of approach and a clear arrangement logic. Instead of suggesting one architecture to adopt in any environment, the study acknowledges that different types of IoT intrusion detection issues are determined by the constraint of deployment used (edge devices need lightweight inference), distribution of those recently deployed areas (needs transfer on the presence of limited label requirements), and autonomous organizations (need privacy-preserving cooperation). The second strength is the application of various benchmark datasets in the field of botnet traffic, DDoS traffic, and heterogeneous IoT traffic environment. The third strength is that there are ablation, sensitivity and complexity analyses as opposed to accuracy reporting only.

LIMITATIONS

It also has limitations on the study. First, the test is based on open benchmarking datasets, which face the same issue of being unable to completely capture continuous drift and protocol diversity in real-world IoT setting. Second, binary neural networks necessarily create limits on representation and the equilibrium between efficiency and accuracy can be made more acute with finer-grained or zero-day attack detection. Third, federated learning presents an orchestration and complexity of systems such as variability in client participation, synchronization costs, as well as security threats of poisoning as well as adversarial updates. Lastly, model interpretability in all three frameworks is not exhaustively good; this is crucial as far as to operational acceptance in security contexts where analysts oftentimes demand clarifications of the usefulness that the alerts provided by the models.

PRACTICAL IMPLICATIONS

To the practitioners, the findings imply a graduated implementation plan. LIIDXC has been used on edgesides or gateway-side sensors where the inference efficiency is

mandatory. EMTD-SSC should be used when the available labeled attack data on a particular site is limited but it can build up on pre-training provided by a similar domain. ID-CFL can be used where various organizations, locations, or groups of devices need to cooperate without any exchange of raw traffic records. The three frameworks thus represent various lifecycle stages of an IoT security program as opposed to mutually exclusive options.

CONCLUSION AND FUTURE WORK

In this paper, the original thesis was transformed into a research article that resembles a journal paper and has three coordinated contributions to the IoT intrusion detection. The paper initially presented LIIDXC a small neural network an XNOR-CNN-LSTM classifier that minimizes calculation-related expenses but does not compromise its classification rates. It subsequently proposed EMTD-SSC, which is a transfer learning model that is resistant to extreme data scarcity in the target domain. Lastly, it presented ID-CFL a federated contrastive learning model that allows collaborative intrusion detection with privacy-preserving scenarios in a heterogeneous setting.

Throughout the experiments, it is found that the findings substantiate the more general statement that the effective design of the IoT IDS needs to take explicitly into account the constraints of operations. Precision is not sufficient when a target system is memory-bound, has poor labels or is decentralized by organization. The suggested frameworks demonstrate that lightweight computation, knowledge transfer and adaptive federated collaboration can augment each of the subsections of the intrusion detection pipeline.

The current research ought to be expanded in at least four directions in the future. To start with, the frameworks must be tested on real-life or longitudinal traffic to determine concept drift resilience. Second, the study of adversarial robustness needs more explicit studies, particularly when dealing with binary and federated scenarios. Thirdly, there is a possibility that multimodal pre-training which is an integration of packet, flow, log and contextual device metadata can enhance generalization to zero-day attacks. Fourth, explainability and user-friendly interfaces need to be combined in such a way that enhanced accuracy would result in more achievable cyber defense.

DECLARATIONS

Acknowledgement: We appreciate the generous support from all the contributors to the research and their different affiliations.
Funding: No funding body in the public, private, or nonprofit sectors provided a particular grant for this research.
Availability of data and material: In the approach, the data sources for the variables are stated.
Authors' contributions: Each author participated equally in the creation of this work.
Conflicts of Interest: The authors declare no conflict of interest.
Consent to Participate: Yes
Consent for publication and Ethical approval: Because this study does not include human or animal data, ethical approval is not required for publication. All authors have given their consent.

REFERENCES

Abdelatey M, Doriguzzi Corin R, Siracusa D. (2021). DAICS: A deep learning solution for anomaly detection in industrial control systems[J]. IEEE Transactions on Emerging Topics in Computing.

Abdi H, Williams L J. (2010). Principal component analysis [J]. Wiley interdisciplinary reviews: computational statistics.

Affinito A, Zinno S, Stanco G, et al. (2023). The evolution of Mirai botnet scans over a six-year period [J]. Journal of Information Security and Applications.

Ahmad Z, Shahid Khan A, Wai Shiang C, et al. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches[J]. Transactions on Emerging Telecommunication Technologies.

Amor N B, Benferhat S, Elouedi Z. (2004). Naïve bayes vs decision trees in intrusion detection systems[C]//Proceedings of the 2004 ACM symposium on Applied computing.

Anderson D, Frivold T, Valdes A. (1995). Next generation intrusion detection expert system (NIDES): A summary[J] SRI Int'l.

Aslan O A, Samet R. (2020). A comprehensive review on malware detection approaches[J]. IEEE access.

Aydin H, Orman Z, Aydin M A. (2022). A long short term memory (LSTM) based distributed denial of service (DDoS) detection and defense system design in public cloud network environment[J]. Computers & Security.

Bandari V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types[J]. International Journal of Business Intelligence and Big Data Analytics.

Beaman C, Barkworth A, Akande T D, et al. (2021). Ransomware: Recent advances, analysis, challenges and future research directions[J]. Computers & security.

Bethge J, Bartz C, Yang H, et al. (2021). Meliusnet: An improved network architecture for binary neural networks [C]//Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision.

Biermann E, Cloete E, Venter L M. (2001). A comparison of intrusion detection systems[J]. Computers & Security.

Bilge L, Dumitras T. (2012). Before we knew it: an empirical study of zero day attacks in the real world[C]//Proceedings of the 2012 ACM conference on Computer and communications security.

Binbusayyis A. (2024). Hybrid VGG19 and 2D-CNN for intrusion detection in the FOG-cloud environment [J].Expert Systems with Applications.

Blakeney C, Yan Y, Zong Z. (2020). Is pruning compression?: Investigating pruning via network layer similarity [C]//Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision.

Blanchard P, El Mhamdi E M, Guerraoui R, et al. (2017). Machine learning with adversaries: Byzantine tolerant gradient descent [J]. Advances in neural information processing systems.

Bouke M A, Abhullah A, ALshatebi S H, et al. (2022). An enhanced intelligent intrusion detection system based on decision tree algorithm[J]. Journal of Applied Artificial Intelligence.

Bourlard H, Kamp Y. (1988). Auto association by multilayer perceptron's and singular value decomposition [J].Biological cybernetics.

Bulat A, Tzimiropoulos G. (1909). Xnor-net++: Improved binary neural networks [J]. arxiv preprint arxiv.

Button K S, Ioannidis J P A, Mokrysz C, et al. (2013). Power failure: why small sample size undermines the reliability of neuroscience [J]. Nature reviews neuroscience.

Chakraborty N. (2013). Intrusion detection system and intrusion prevention system. A comparative study[J]. International Journal of Computing and Business Research (IJCBR).

Chen D, Zhang F, Zhang X. (2022). Heterogeneous IoT Intrusion Detection Based on Fusion Word Embedding Deep Transfer Learning [J]. IEEE Transactions on Industrial Informatics.

Chhabra S, Majumdar P, Vatsa M, et al. (2019). Data fine tuning [C]//Proceedings of the AAAI Conference on Artificial Intelligence.
Creswell A, White T, Dumoulin V, et al. (2018). Generative adversarial networks: An overview [J]. IEEE signal processing magazine.
Debar H, Curry D, Feinstein B. (2007). The intrusion detection message exchange format (IDMEF)[R].
Debicha I, Bauwens R, Debatty T, et al. (2023). TAD: Transfer learning based multi adversarial detection of evasion attacks against network intrusion detection system [J]. Future Generation Computer Systems.
Deng A, Hooi B. (2021). Graph neural network based anomaly detection in multivariate time series [C]//Proceedings of the AAAI conference on artificial intelligence.
Feinstein B, Matthews G. (2007). The Intrusion Detection Exchange Protocol (IDXP)[J].
Fu B, Liu Y, Wang Y, et al. (2023). IQR-MAD Based Anomaly Detection of Voltage Data in the Distribution Network [C]//2023 6th International Conference on Energy, Electrical and Power Engineering (CEEPE).IEEE.
Garcia S, Parmisano A, Erquiaga M J. (2020). A labeled dataset with malicious and benign IoT network traffic [J]. Stratosphere Lab, Praha Czech Republic, Tech, Rep.
Goodge A, Hooi B, Ng S K, et al. (2021). Robustness of autoencoders for anomaly detection under adversarial impact [C]//Proceedings of the twenty ninth international conference on international joint conferences on artificial intelligence.
Gou J, Yu B, Maybank S J, et al. (2021). Knowledge distillation: A survey [J]. International Journal of Computer Vision.
Gracia-Teodoro P, Diaz-Verdejo J, Macia-Fernandez G, et al. (2009). Anomaly based network intrusion detection: Techniques, systems and challenges[J]. Computers & Security.
Graves A, Graves A. (2012).Long Short Term Memory [J].Supervised sequence labelling with recurrent neural networks.
Gu J, Lu S. (2021). An effective intrusion detection approach using SVM with naïve Bayes feature embedding[J]. Computers & Security.
Han D, Wang Z, Chen W, et al. (2021). Deepaid: Interpreting and improving deep learning based anomaly detection in security applications [C]//Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security.
Heidari A, Jabraeil Jamali M A. (2023). Internet of Things intrusion detection systems: a comprehensive review and future directions[J]. Cluster Computing.
Jin X, Xie Y, Yin Y. (2021). BotCatcher: A Complementary Advantages and Deep Learning Based Scheme for Intrusion Detection [C]//2021 13th International Conference on Intelligent Human Machine Systems and Cybernetics (IHMSC). IEEE.
Karimireddy S P, Kale S, Mohri M, et al. (2020). Scaffold: Stochastic controlled averaging for federated learning [C]//International conference on machine learning. PMLR.
Khoa T V, Hoang D T, Trung N L, et al. (2022). Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks [J]. IEEE Internet of Things Journal.
Kim G, Kim J, Han B. (2021). Communication efficient federated learning with acceleration of global momentum [J]. arxiv.
Kimura H, Emura K, Isobe T, et al. (2023). A Deeper Look into Deep Learning Based Output Prediction Attacks Using Weak SPN Block Ciphers [J]. Journal of Information Processing.
Kingma D P, Welling M. (2013).Auto encoding varaitional bayes [J].arxiv preprint arxiv.
Koroniotis N, Moustafa N, Sitnikova E, et al. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-iot dataset [J]. Future Generation Computer Systems.
Li J, Zhang J, et al. (2023). Quantum KNN classification with K Value selection and neighbor selection [J]. IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems.
Li T, Sahu A K, Zaheer M, et al. (2020). Federated optimization in heterogeneous networks [J].Proceedings of Machine learning and systems.
Lidemann B, Maschler B, Sahlab N, et al. (2021). A survey on anomaly detection for technical systems using LSTM networks [J]. Computers in Industry.

Lima M F, Zarpelao B B, Sampaio L D H, et al. (2010). Anomaly detection using baseline and k means clustering [C]//SofCOM 2010, 18th International Conference on Software, Telecommunications and Computer Networks.

Liu H, Lang B. (2019). Machine learning and deep learning methods for intrusion detection systems: A survey[J]. applied sciences.

Longari S, Valcarcel D H N, Zago M, et al. (2020). CANnolo: An anomaly detection system based on LSTM autoencoders for controller area network [J]. IEEE Transactions on Network and Service Management.

Lopez Martin M, Sanchez Esguevillas A, Arribas J I, et al. (2022). Supervised contrastive learning over prototype label embedding for network intrusion detection [J].Information Fusion.

Lu H, Wang T, Xu X, et al. (2021). Cognitive memory guided autoencoder for effective intrusion detection in internet of things [J]. IEEE Transactions on Industrial Information's.

Lunt T F, Jagannathan R. (1988).A prototype real time intrusion detection expert system[C]//IEEE Symposium on Security and Privacy.

Lyu M, Gharakheili H H, Sivaraman V. (2024). A survey on enterprise network security: Asset behavioral monitoring and distributed attack detection[J]. IEEE Access.

Madakam S, Ramaswamy R, Tripahti S. (2015). Internet of Things (IoT): A literature review (J). Journal of Computer and Communications.

Mahdavi E, Fanian A, Mirzaei A, et al. (2022). ITL-IDS: Incremental transfer learning for intrusion detection systems [J]. Knowledge based systems.

Maheswari K G, Siva C, Nalinipriya G. (2023). Optimal Cluster based feature selection for intrusion detection system in web and cloud computing environment using hybrid teacher learning optimization enables deep recurrent neural network [J]. Computer Communications.

Makhoul J, Roucos S, Gish H. (1985). Vector quantization in speech coding [J].Proceedings of the IEEE.

Mehedi S T, Anwar A, Rahman Z, et al. (2022). Dependable intrusion detection system for IoT: A deep transfer learning based approach [J]. IEEE Transactions on Industrial Informatics.

Meidan Y, Bohadana M, Mathov Y, et al. (2018). N-Baiot network based detection of iot botnet attacks using deep autoencoders [J]. IEEE Pervasive Computing.

Moudoud H, Mlika Z, Khoukhi L, et al. (2022). Detection and prediction of fdi attacks in iot systems via hidden markov model[J]. IEEE Transactions on Network Science and Engineering.

Muhammad G, Hossain M S, Garg S. (2020). Stacked autoencoder based intrusion detection system to combat financial fraudulent [J]. IEEE Internet of Things Journal.

Muhati E, Rawat D B. (2021). Hidden Markov model enabled prediction and visualization of vyber agility in IoT era[J]. IEEE Internet of Things Journal.

Nevat I, Divakaran D M, Nagarajan S G, et al. (2017). Anomaly detection and attribution in networks with temporally correlated traffic[J]. IEEE/ACM Transactions on Networking.

Ng A. (2011). Sparse autoencoder [J]. CS294A Lecture notes.

Ogheneovo E E, Nlerum P A. (2020). Iterative dichotomizer 3 (ID3) decision tree: A machine learning algorithm for data classification and predictive analysis [J]. International Journal of Advanced Engineering Research and Science.

Ord Kahn C, Porras P A, Staniford-Chen S, et al. (1998). A common intrusion detection framework[J]. Journal of Computer Security.

Palihawadana C, Wiratunga N, Wijekoon A, et al. (2022). Fedsim: Similarity guided model aggregation for federated learning [J]. Neurocomputing.

Pan S J, Yang Q. (2009). A survey on transfer learning [J]. IEEE Transactions on knowledge and data engineering.

Parwez M S, Rawat D B, Garuba M. (2017). Big data analytics for user activity analysis and user anomaly detection in mobile wireless network [J]. IEEE Transactions on Industrial Informatics.

Patel K, Chudasam D. (2021).National Security Threats in Cyberspace (J).National Journal of Cyber Security Law.

Pingale S V, Sutar S R. (2022). Remora whale optimization based hybrid deep learning for network intrusion detection using CNN features [J]. Expert Systems with Applications.
Raj S, Ramanathan L, Kamsin I F B. (2022). Enhancing Data Privacy and Security of Artificial Intelligence in Combating World Hunger[J]. Journal of Applied Technology and Innovation
Rastegari M, Ordonez V, Redmon J, et al. (2016). Xnor-net: Imagenet classification using binary convolutional neural networks [C]//European conference on computer vision. Cham: Springer International Publishing.
Raudys S J, Jain A K. (1991). Small sample size effects in statistical pattern recognition: Recommendations for practitioners [J]. IEEE Transactions on pattern analysis and machine intelligence.
Reddy D K K, Behera H S, Nayak J, et al. (2021). Deep neural network based anomaly detection in Internet of Things network traffic tracking for the applications on future smart cities [J]. Transactions on Emerging Telecommunications Technologies.
Rescorla E. (2003). Security Holes… Who Cares? [C]//12th USENIX Security Symposium (USENIX Security 03).
Rumelhart D E, Hinton G E, Williams R J. (1986). Learning representations by back propagating errors [J].nature
Safara F, Souri A, Serrizadeh M. (2020). Improved intrusion detection method for communication networks using association rule mining and artificial neural networks [J].IET Communications.
Saheb M C P, Yadav M S, Babu S, et al. (2021). A review of DDoS evaluation dataset: CICDDOS2019 dataset [C]//International Conference on Energy Systems, Drives and Automations. Singapore: Springer Nature Singapore.
Schuster M, Paliwal K K. (1997). Bidirectional recurrent neural networks [J].IEEE transactions on Signal Processing.
Seo E, Song H M, Kim H K. (2018). GIDS: GAN based intrusion detection system for in vehicle networks [C]//2018 16th annual conference on privacy, security and trust (PST).
Shang F, Cheng J, Liu Y, et al. (2017). Bilinear factor matrix norm minimization for robust PCA: Algorithms and applications[J]. IEEE transactions on pattern analysis and machine intelligence.
Singh N B, Singh M M, Sarkar A, et al. (2021). A novel wide & deep transfer learning stacked GRU framework for network intrusion detection [J]. Journal of Information Security and Applications.
Singh P, Kaur A, Aujla G S, et al. (2020). Daas: Dew computing as a service for intelligent intrusion detection in edge of things ecosystem [J]. IEEE Internet of Things Journal.
Sinha D, El-Sharkawy M. (2019). Thin mobilenet: An enhanced mobilenet architecture [C]//2019 IEEE 10th annual ubiquitous computing, electronics & mobile communication conference (UEMCON).
Siniosoglou I, Radoglou Grammatikis P, Efstathopoulos G, et al. (2021). A unified deep learning anomaly detection and classification approach for smart grid environments [J]. IEEE Transactions on Network and Service Management.
Sivanantham S, Mohanraj V, Suresh Y, et al. (2023). Association Rule Mining Frequent Pattern Based Intrusion Detection in Network [J]. Computer Systems Science & Engineering.
Slaon R, Warner R. (2017). Unauthorized access: The crisis in online privacy and security [M]. Taylor & Francis.
Staniford-Chen S, Cheung S, Crawford R, et al. (1996). Gr IDS-a graph based intrusion detection system for large networks[C]//Proceedings of the 19th national information systems security conference.
Sun H, Chen M, Weng J, et al. (2021). Anomaly detection for in vehicle network using CNN LSTM with attention mechanism [J].IEEE Transactions on Vehicular Technology.
Sun P, Liu P, Li Q, et al. (2020). DL-IDS: Extracting Features Using CNN-LSTM Hybrid Network for Intrusion Detection System [J]. Security and communication networks.
Tang W, Hua G, Wang L. (2017). How to train a compact binary neural network with high accuracy? [C]//Proceedings of the AAAI conference on artificial intelligence.

Tian Y, Sun C, Poole B, et al. (2020). What makes for good views for contrastive learning? [J]/ Advances in neural information processing systems.
Vaiyapuri T, Algamdi S, John R, et al. (2023). Metaheuristics with federated learning enabled intrusion detection system in Internet of Things environment[J]. Exper Systems.
Vaiyapuri T, Binbusayyis A. (2020). Application of deep autoencoder as an one class classifier for unsupervised network intrusion detection: a comparative evaluation [J]. PeerJ Computer Science.
Wang H, Wen J, Liu J, et a. (2023). ACKE: Asymmetric Computing Key Exchange Protocol for IoT Environments [J]. IEEE Internet of Things Journal
Wang T, Qiao M, Lin Z, et al. (2018). Generative neural networks for anomaly detection in crowded scenes [J].IEEE Transactions on Information Forensics and Security.
Wazirali R. (2020). An improved intrusion detection system based on KNN hyper parameter tuning and cross validation [J]. Arabian Journal for Science and Engineering.
Wu J, Wang Y, Xie B, et al. (2022). Joint semantic transfer network for IoT intrusion detection [J].IEEE Internet of Things Journal.
Yang J, Deng J, Li S, et al. (2017). Improved traffic detection with support vector machine based on restricted Boltzmann machine [J]. Soft Computing.
Yifeng WANG, Yuanbo GUO, Qingli CHEN, Chen FANG, Renhao LIN. (2022). Method based on contrastive learning for fine grained unknown malicious traffic classification [J]. Journal on Communications.
Yilmaz S, Aydogan E, Sen S. (2021). A transfer learning approach for securing resource constrained IoT devices [J]. IEEE Transactions of Information Forensics and Security.
Yin C, Zhang S, Wang J, et al. (2020). Anomaly detection based on convolutional recurrent autoencoder for IoT time series [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems.
Yin Y, Jang Jaccard J, Xu W, et al. (2023). IGRF-RFE: a hybrid feature selection method for MLP based network intrusion detection on UNSW-NB15 dataset [J]. Journal of Big Data.
You K, Long M, Cao Z, et al. (2019).Universal domain adaptation [C]//Proceedings of the IEEE / CVF conference on computer vision and pattern recognition.
Zhang S S, Yu T, Chen G M. (2017). Reinforced concrete beams strengthened in flexure with near surface mounted (NSM) CFRP strips: Current status and research needs[J]. Composites Part B: Engineering.
Zhang X, Zhao R, Jiang Z, et al. (2024). AOC-IDS: Autonomous Online Framework with Contrastive Learning for Intrusion Detection [J]. arxiv preprint arxiv.
Zhou K, Liu Z, Qiao Y, et al. (2022). Domain generalization: A survey [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence.
Zhou X, Hu Y, Liang W, et al. (2020). Variational LSTM enhanced anomaly detection for industrial big data [J]. IEEE Transactions on Industrial Information's.
Zhu H, Xu J, Liu S, et al. (2021). Federated learning on non-IID data: A survey [J]. Neurocomputing.
Zuo C, Lin Z, Zhang Y. (2019). Why does your data leak? Uncovering the data leakage in cloud from mobile apps[C]//2019 IEEE Symposium on Security and Privacy (SP).