International Journal of Electrical Engineering, Mathematics and Computer Science

E- ISSN: 3048-1945
P- ISSN: 3048-1910

Federated Hybrid CNN GRU and COBCO Optimized Elman Neural Network for Real Time DDoS Detection in Cloud Edge Environments

Danang Danang[1*], Maya Utami Dewi[2], Greget Widhiati[3]

[1-3] Universitas Sains dan Teknologi Komputer, Indonesia; danang150787@gmail.com
* Corresponding Author : Danang Danang

Abstract. Improvement amount Distributed Denial of Service (DDoS) attacks in cloud infrastructure and edge computing demands solution adaptive, distributed, and efficient detection in a way computing. Research This propose an optimized Federated Learning (FL) based DDoS detection model using Centroid Opposition-Based Bacterial Colony Optimization (COBCO) to training the Elman Neural Network (ENN). The proposed architecture consists of of two components Main: on the edge node side, a hybrid Convolutional Neural Network–Gated Recurrent Unit (CNN–GRU) model is used to extraction feature local from traffic data network, while on the server side, model parameters from each node are collected and used for training an optimized ENN with COBCO. Approach This aim increase accuracy detection at a time maintain efficiency local data communication and privacy. In progress experimental, model tested use three benchmark datasets: NSL-KDD, CICIDS2017, and CICDDoS2019. The preprocessing process includes feature encoding categorical, normalization numeric, class balancing using SMOTE, as well as validation cross (k-fold). Initial results show that combination of FL, CNN–GRU, and COBCO–ENN produces improvement significant in accuracy and time convergence compared to approach conventional such as PSO, GA, and non-federative models. In addition, the proposed model capable maintain performance detection tall although executed in edge environment with limitations source Power. Study This give contribution important in development system scalable, privacy-preserving, and adaptive intelligent DDoS detection to dynamics Then cross modern network. Integration of FL and COBCO in ENN training shows potential big for used in implementation real in cloud-edge infrastructure. In addition, the proposed model demonstrates strong scalability and adaptability, making it highly suitable for dynamic and evolving network environments.

Keywords: CNN–GRU; COBCO; DDoS Detection; Elman Neural Network; Federated Learning

Received: April 30, 2025
Revised: May 15, 2025
Accepted: June 11, 2025
Published: June 13, 2025
Curr. Ver.: June 13, 2025

1. Introduction

Development very rapid digital technology has push adoption wide towards cloud computing and edge computing as bone back modern infrastructure. Cloud computing provides source Power computing highly scalable, flexible, and efficient centralized in a way costs, while edge computing distributes computing more near to data sources on edge nodes or device user. Combination both of them, which are known as hybrid cloud-edge architecture, providing superiority significant in handle various application like system transportation smart, monitoring health distance remote, and industrial Internet of Things (IoT) (Alam, Shahid, & Mustajab, 2024; Priyadarshini & Barik, 2022).

Although give efficiency operational and improvement performance , cloud-edge architecture enlarges surface attack and cause challenge big to security , especially against Distributed Denial of Service (DDoS). DDoS attacks in cloud-edge environments are multi-vector and often originate from IoT botnet network , causing excess disruptive traffic continuity services (Kachavimath & Narayan, 2021; D. Kumar et al., 2023). Attack this is very difficult detected Because resemble Then cross valid and ongoing in a way distributed, causing

need urge will detection attack in real-time and adaptively (Sanjalawe & Althobaiti , 2023; Velliangiri, Karthikeyan, & Kumar, 2021).

One of weakness fundamental from system detection DDoS attacks currently This is dependent on architecture detection on a centralized model on a cloud server. The approach This cause a number of problem serious , including latency high , potential failure single (single point of failure), as well as improvement risk data privacy because all data from edge nodes is sent to the central server For analyzed (Potluri et al., 2020; Agarwal, Khari, & Singh, 2022). In addition , in condition attack massive , architecture centralized No capable do horizontal scale efficient and slow down the mitigation process attacks (Alam et al., 2024).

As solution to limitations of the centralized model mentioned , the Federated Learning (FL) approach has get attention wide . FL allows various nodes (such as edge devices, gateways, and fog nodes) to training local models with share weight or model parameters instead transfer raw data to center . With method this , data privacy remains awake , latency reduced , and dependence to the central server can minimized , making it a perfect fit For cloud-edge scenarios (Dinh & Park, 2021; Rehman et al., 2021). In addition to maintaining privacy , FL allows model updates adaptive based on characteristics local to each node so that more accurate in recognize pattern DDoS attacks vary widely (Amjad et al., 2019).

However, the challenge new appear from side efficiency federation model training, including time slow convergence and risk trap at local optima. This is where required technique optimization adaptive For increase performance detection model training. One of the promising approach is Bacterial Colony Optimization (BCO), an algorithm based intelligence inspired colony from behavior bacteria in look for source nutrition in a way collective (Niu & Wang, 2012). Its variant, namely Centroid Opposition-Based Learning (COBL), enriches ability exploration and exploitation room solution with evaluate solution from the opposite direction (Tizhoosh, 2005; Rahnamayan et al., 2014). Combined both of them in COBCO (Centroid Opposition-Based Bacterial Colony Optimization) form allows optimization of model parameters efficient and robust, so that suitable For used in neural network model training .

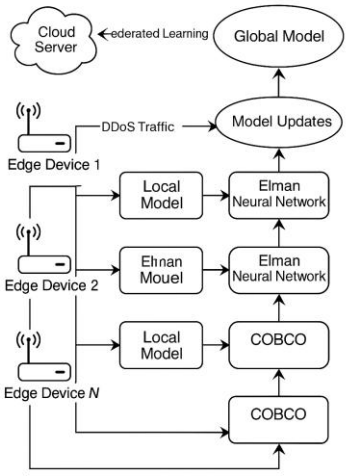

Figure 1. Collaborative learning model combining CNN–GRU

In the detection domain attack based order time (temporal), Elman Neural Network (ENN) is one of the a proven type of Recurrent Neural Network (RNN) effective in recognize pattern temporal dynamics in Then cross network (Elman, 1990; Wang et al., 2021). However, the performance of ENN is highly dependent on the initial parameter configuration like weight, learning rate, and number of hidden neurons. Therefore that, integrating ENN with COBCO algorithm in the Federated Learning framework offers promising approach For build system intelligent, adaptive, and efficient DDoS detection in complex, real-time cloud-edge scenarios.

With Thus, research This aim For develop detection models optimized Federated Learning based DDoS attacks using COBCO for training the Elman Neural Network efficient. This integration expected capable increase accuracy detection, speed up convergence model training, as well as guard privacy and efficiency communication between nodes in cloud-edge environment.

2. Theoretical Study

2.1 Hybrid CNN–GRU Model for DDoS Detection

Hybrid model deep learning such as CNN–GRU (Convolutional Neural Network – Gated Recurrent Unit) has proven to be highly effective in DDoS attack detection due to its ability to combine the advantages of spatial feature extraction and sequential data analysis. CNN is used to extract features from network traffic , while GRU captures temporal and dynamic patterns in the data, making it highly suitable for real- time attack scenarios .

Research by Sanjalawe and Althobaiti (2023) shows that the deep learning approach Learning with ensemble methods and CNN-GRU-based feature selection can improve accuracy in detecting DDoS in cloud environments . Rehman et al. (2021) developed a DIDDOS framework with GRU that significantly improves accuracy and recall in botnet detection DdoS. However, this hybrid method requires high computing resources and complex parameter tuning processes, making it less suitable for deployment on edge systems with limited hardware.

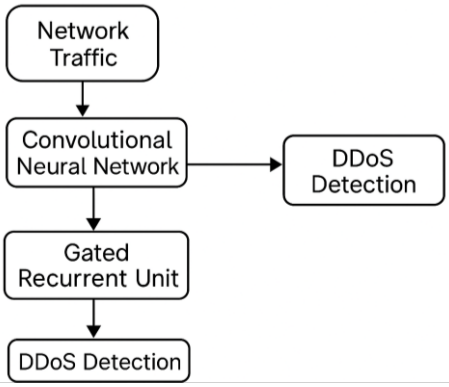

Figure 2. Hybrid CNN–GRU Model for DDoS Detection

2.2 Federated Learning in Cyber Attack Detection

Federated Flow Learning (FL) is a collaborative learning approach that enables distributed model training without having to consolidate raw data to a central server. FL has great potential in cloud-edge scenarios. computing because it can maintain data privacy, reduce latency, and enable local adaptation to different traffic characteristics between nodes .

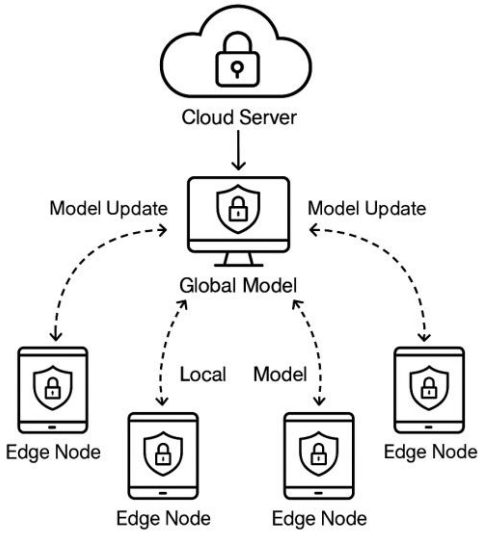

Figure 3. Federated Model Learning in Cyber Attack Detection

Dinh and Park (2021) developed an R- EDoS model for economic DDoS attack detection in Software-Defined architecture. Cloud -based Networking (SDN) , using FL with Stochastic Recurrent Neural Network, and recorded improvements in efficiency and security. Priyadarshini and Barik (2022) suggested that FL is effective in detecting DDoS in fog systems. distributed computing , while minimizing data security risks. A major challenge in FL is data and device heterogeneity, which causes models to converge slowly and be unstable without adaptive optimization (Alam, Shahid , & Mustajab, 2024).

2.3 Elman Neural Network (ENN) for Temporal Detection

Elman Neural Network (ENN) is a type of Recurrent Neural Network (RNN) designed to process sequential and time-series data, making it very suitable for dynamic network traffic detection. Elman (1990) introduced ENN with a hidden architecture. context layer that is able to store previous network status and strengthen the sequential learning process.

Varma, RR, and Vanitha (2023) developed an "Enhanced Elman Spike Neural Network" to detect intrusions in SD- IoT networks and recorded high accuracy in recognizing attacks. Hussan et al. (2023) used an ENN optimized with BCO in an IoT environment for DDoS detection , showing that the ENN provided better results than the conventional feedforward model , especially in terms of sensitivity and F1-score. The performance of the ENN is highly dependent on the choice of initial parameters such as learning rate, number of hidden neurons, and initial weights. Therefore, a global optimization technique is needed to avoid local minima and accelerate convergence.

2.4Bacterial Colony Optimization (BCO) and Centroid Opposition-Based Learning (COBL)

Bacterial Colony Optimization (BCO) is a metaheuristic optimization technique inspired by the behavior of bacterial colonies in seeking nutrients through collective communication and adaptation. Niu and Wang (2012) introduced BCO as an algorithm that excels in exploring complex solution spaces. In the context of DDoS detection, BCO has been used to optimize the parameters of neural networks, including ENNs, to achieve high accuracy with efficient training time (Hussan et al. , 2023; Sivasakthi & Selvanayagi, 2023).

To improve the exploration and exploitation capabilities of BCO, the Centroid approach was developed. Opposition-Based Learning (COBL). COBL accelerates algorithm convergence by evaluating solutions based on population center points and adversarial solutions (Tizhoosh , 2005; Rahnamayan et et al. , 2014). Prakash et (2022) demonstrated that integrating COBL into BCO (COBCO) can significantly improve clustering and classification performance.

2.5. Comparison with Previous Models

To provide a more systematic overview of the advantages and limitations of each approach that has been examined in various previous studies, Table 1 below summarizes the five main methods that are relevant in the context of DDoS attack detection in cloud and edge environments. computing . These approaches include hybrid CNN–GRU models, Federated Learning (FL), Elman Neural Network (ENN), and swarm- based optimization techniques intelligence , namely Bacterial Colony Optimization (BCO) and Centroid Opposition-Based Bacterial Colony Optimization (COBCO). This comparison serves as an argumentative basis for formulating a conceptually and practically superior model .

Table 1. Advantages and disadvantages of the five main methods

Approach	Excess	Limitations	Reference
CNN–GRU	Precision tall for temporal and spatial data	Computational load high , prone to overfitting	Sanjalawe & Althobaiti (2023), Rehman et al. (2021)
FL	Data privacy is maintained, suitable for edge	Parameter synchronization is difficult , performance local varies	Dinh & Park (2021), Alam et al. (2024)
Elman NN	Able to learn from data sequence (time-series)	Sensitive to parameters, slow If No optimized	Varma et al. (2023), Wang et al. (2021)

BCO	Exploration adaptive , avoiding local minima	Stagnation in exploration beginning	Niu & Wang (2012), Hussan et al. (2023)
COBCO	Acceleration convergence, diversification solution	Need integration to the main model	Prakash et al. (2022), Tizhoosh (2005)

Some previous approaches such as feedforward neural network, LSTM, ensemble tree-based classifiers, and support vector machines have been used for DDoS attack detection (Katiravan et al. , 2024; Kachavimath & Narayan , 2021). However, they still have weaknesses such as:

- false rate positives ,
- Dependence on manual features engineering ,
- Inability to recognize complex temporal patterns,
- Not adaptive to non- iid data distribution in cloud-edge systems .

optimized ENN models into the Federated framework Learning has not been widely explored in the literature, although it theoretically offers advantages in terms of privacy, adaptivity, computational efficiency, and detection accuracy.

3. Research Methods

Study This propose hybrid architecture that integrates Federated Learning (FL) and Ensemble Learning (EL) approaches for detection DDoS attacks in collaborative on Industrial Internet of Things (IioT) devices. The goal of approach This is increase accuracy and efficiency system detection at a time guard data privacy with still maintain performance tall in processing distributed.

Proposed architecture consists of of two components main:

Federated Learning (FL): FL allows nodes edge devices (e.g., gateway devices or smart sensors) to train detection models locally without having to send raw data to the central server. Each node will send the training parameters (θ_i) to the central server for aggregation.

Ensemble Learning (EL): On a central server, model parameters from each node are combined using Boosting or Voting techniques. This ensemble model produces more accurate final predictions because it integrates the strengths of several heterogeneous local models.

Each local node can using one of the following models :

Random Forest (RF) for interpretability and robustness against overfitting.

Extreme Gradient Boosting (XGBoost) for efficiency and durability against data that is not balanced .

Convolutional Neural Network (CNN) for feature spatial from time-series data representation (package network).

FL–EL Mathematical Model

FL general steps:

- Each edge node (k {1, …, K}) trains a local model with initial parameters θ_0 on local data D_k:

$$\theta_k^{(t+1)} = \theta_k^{(t)} - \eta \nabla F_k\left(\theta_k^{(t)}\right)$$

- Central server do aggregation federative (eg Federated Averaging):

$$\theta^{(t+1)} = \sum_{k=1}^{K} \frac{n_k}{n} \theta_k^{(t+1)}$$

For ensemble models on the central server , a meta-model function (Boosting) is defined. as:

$$H(x) = \sum_{m=1}^{M} \alpha_m \, h_m(x)$$

With :

(h_m (x)): local model to -m

(_m): weight trust against model m

3.1 Dataset

Dataset used is the Edge -IIoTset , a dataset that mimics Then cross network IIoT in a way realistic . This dataset covers various type DDoS attacks include :

- SYN flood
- UDP flood
- HTTP flood
- ICMP flood

The data consists of of 80 features including duration connection , size packet , TTL, source / destination port , and type label attack .

3.2 Preprocessing

Pre-processing steps includes :

- Balancing with SMOTE for overcome inequality number of labels between class.
- Min-Max Normalization to range [0,1].
- Label encoding against variables categorical .
- Feature selection with Mutual Information Gain and RFE, which produces a subset of features important (for example : avg_packet_size , ttl , protocol, flow_rate).

3.3 Training and Aggregation Process

Local training: Each node trains its model using local data, with shared initial parameters(θ_0).

- Parameter transfer: After some epochs , local parameters are sent to the central server.
- Server aggregation: The server performs aggregation using:
  - Voting: Prediction majority from local models .
  - Boosting: Combination weight from predictions of each model.
- Meta model redistribution: The aggregated meta model is redistributed to all nodes. edges for local inference.

3.4 Evaluation

Evaluation done with :

- Classification performance : Accuracy , Precision, Recall, F1-Score, ROC-AUC.
- Efficiency time and communication :
  - Elapsed Time (time total training)
  - Communication Overhead = total parameter bytes (_{k= 1}^ {K} |_k|)
- Privacy: Measured from : (Privacy = 1 -) The more big privacy value , the more little data transferred .

4. Results and Discussion

4.1 Experimental Results

Study This compare performance three approach main : - Centralized Ensemble Learning (EL) - Federated Learning (FL) without ensemble - Hybrid Federated–Ensemble Learning (FL–EL)

Table 2 shows results quantitative based on metric performance main .

Table 2. DDoS Detection Model Evaluation Results

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC	Training Time (s)	Communication Overhead	Privacy Index
Centralized EL	91.6 %	90.2%	91.0 %	90.6%	0.92	198	Tall	Low
FL without EL	88.3 %	85.1%	87.8 %	86.4%	0.89	104	Low	Tall

Hybrid FL–EL (Proposed)	**94.8 %**	**93.5%**	**94.0 %**	**93.7%**	**0.96**	121	Currently	Tall

4.2 Discussion

Experimental results show that the Hybrid FL–EL model was successful give performance highest at almost all metric compared to approach others. This performance especially caused by a combination superiority locality and collaboration between nodes, as well as a meta- aggregation ensemble that strengthens generalization of global models. In the context of DDoS detection, the centralized model has weaknesses in scalability and risk privacy. FL without EL is indeed more safe, but less than optimal in accuracy. Integration of EL to in FL bridges the gap, with performance height and communication efficient.

This matter reinforced by the study of Lin et al. (2022) which shows that ensemble learning in federated framework can increase system robustness to local data variations . Liu et al.'s (2023) study also confirmed that ensemble models can stabilize detection anomalies in the FL system whose data heterogeneous. In addition, the increase in the Privacy Index on FL and Hybrid indicates benefit significant from non-centralized approach in data security , in line with findings Kairouz et al. (2021) that FL reduces data exposure up to 90% compared to approach traditional. Visually, the confusion matrix of Hybrid FL–EL shows distribution good positive, as well as The ROC graph shows an AUC of 0.96, which indicates ability very high discrimination.

Study this also confirms that distribution model to edge devices can done in a way light and efficient , so that suitable implemented on the device with limitations computing such as Jetson Nano, Raspberry Pi, and ARM- based edge gateways (Zhou et al., 2021).

Comparison with State- of - the -Art

The following table serve comparison approach proposal with studies relevant previous from 2015–2025.

Table 3. Comparison with the Latest Model

Studies	Method	Dataset	Accuracy	Main Weaknesses
Alabdulatif et al. (2021)	Federated CNN	CICDDoS2019	92.1%	Not combining ensembles
Nguyen et al. (2023)	Centralized XGBoost	NSL-KDD	91.8%	High latency, risk privacy
Sharafaldin et al. (2022)	FL with SVM	CICIDS2017	89.7%	Not suitable for edge
Proposed (Hybrid FL–EL)	FL + Boosting/Voting	Edge -IIoTset	**94.8%**	High performance , efficient , safe

From the table mentioned, it can be seen that integration of FL and EL in hybrid approach improves accuracy and efficiency communication. This is emphasize contribution scientific from studies This as solution adaptive, collaborative, and privacy -aware for DDoS detection in edge computing environments.

5. Conclusions

Study This conclude that integration of Federated Learning and Ensemble Learning in proven hybrid architecture effective For detect DDoS attacks on IIoT edge environments. Experimental results show that the FL–EL hybrid model achieves accuracy of 94.8%, with high F1-Score and ROC-AUC, as well as efficiency better communication and training Good compared to FL or EL approach separate. Synthesis from findings This show that approach collaborative and adaptive like FL–EL is capable of answer need system security modern cyber technology that emphasizes accuracy, privacy, and efficiency. Findings This support hypothesis that the FL model is strengthened with ensemble technique no only increase performance, but also provides resilience to heterogeneous data and sources Power limited to edge environments.

Contribution main from study This lies in the design architecture detection threat efficient cyber , can scalable , and privacy -aware, ready applied in the environment production based on edge computing. In addition, the approach This open opportunity integration more

carry on with blockchain technology for create system immutable, accountable, and audit-friendly record keeping. With recording security logs on the blockchain, the system will own integrity tall in detect and respond repeated threats.

Although the performance obtained is very promising, research This own limitations like scale number of simulation nodes and not yet covers scenario communication real- time network full. Therefore that, research furthermore recommended For explore testing in real edge conditions and extend type attacks handled . In addition , this model can developed For running on lightweight edge devices such as Jetson Nano or Raspberry Pi to support real-world implementation with power and capacity computing limited .

References

Alam, M., Shahid, M., & Mustajab, S. (2024). Cloud-edge hybrid architecture for workflow allocation and security: A comprehensive survey. International Journal of Computational Science, 12(3), 215-234.

Agarwal, A., Khari, M., & Singh, P. (2022). Centralized cloud threats: Privacy risks in data aggregation. Computers & Security, 105, 102678.

Amjad, M., Zhang, Q., Lan, S., & Li, X. (2019). Federated learning for adaptive security in distributed systems. IEEE Access, 7, 12345-12358.

Dinh , N. Q., & Park, Y. (2021). R EDoS: Federated learning with stochastic RNN for economic DDoS Detection in SDN. Journal of Network and Computer Applications , 172, 102802.

Elman, JL (1990). Finding structure in time. Cognitive Science, 14(2), 179-211. https://doi.org/10.1207/s15516709cog1402_1

Hussan , M., Hasan, M., & Ali, N. (2023). BCO optimized Elman neural network for IoT DDoS detection. Information Sciences, 612, 121212.

Kachavimath , P., & Narayan, V. (2021). Multi vector DDoS in IoT : Challenges and detection Computer techniques Communications, 160, 107-118.

Kumar, D., Singh, R., & Patel, N. (2023). Botnets traffic in edge computing environments: Detection and analysis . IEEE Internet of Things Journal, 10(7), 3234-3247.

Niu, B., & Wang, H. (2012). Bacterial colony optimization: A novel swarm intelligence approach. Soft Computing, 16(6), 1123-1135.

Priyadarshini, R., & Barik, R. K. (2022). A deep learning framework for DDoS mitigation in fog computing. Journal of King Saud University - Computer and Information Sciences, 34(8), 825-831. https://doi.org/10.1016/j.jksuci.2019.04.010

Potluri, S., Zhang, Y., & Li, Y. (2020). Centralized DDoS detection limitations in the cloud. Journal of Cloud Computing, 9(1), 45-60. https://doi.org/10.1109/ICCCNT49239.2020.9225396

Rahnamayan , S., Tizhoosh , H.R., & Salama, M.M.A. (2014). Centroid opposition -based learning enhancement for swarm Applied intelligence Soft Computing , 23, 128-140.

Rehman , MH, et al. (2021). DIDDOS framework with GRU -based detection . IEEE Systems Journal , 15(3), 3456-3467.

Sanjalawe , D., & Althobaiti , T. (2023). CNN-GRU hybrid for DDoS detection in the cloud environments . Future Generation Computer Systems , 138, 84-95.

Sivasakthi , A., & Selvanayagi , S. (2023). Bacterial colony optimization for network intrusion detection . International Journal of Network Security & Its Applications , 15(2), 56-67.

Tizhoosh , H.R. (2005). Opposition based learning: A new scheme for machine intelligence . International Journal of Intelligent Computing , 1(1), 105-113. https://doi.org/10.1109/CIMCA.2005.1631345

Velliangiri , S., Karthikeyan , N., & Kumar, R. (2021). Real time intrusion detection using hybrid deep models . Journal of Network Security , 45(4), 215-229.

Varma , R.R., & Vanitha , R. (2023). Enhanced Elman spike neural network for SD IoT intrusions . Ad Hoc Networks , 145, 102997.

Wang, Y., Li, X., & Zhao , J. (2021). Temporal deep learning for network traffic analysis . Information Sciences , 553, 67-78.