Comparative Evaluation of Cloud–Edge Security Architectures for DDoS Detection

Mustafa Furkan Ceylan
Department of Computer Engineering
Dokuz Eylül University
Balıkesir University
İzmir & Balıkesir, Turkey
0009-0005-5609-395X

Gökhan Dalkılıç
Department of Computer Engineering
Dokuz Eylül University
İzmir, Turkey
0000-0002-0130-1716

Mehmet Hilal Özcanhan
Department of Computer Engineering
Dokuz Eylül University
İzmir, Turkey
0000-0002-5619-6722

2025 18th International Conference on Information Security and Cryptology (ISCTürkiye) | 979-8-3315-5709-6/25/$31.00 ©2025 IEEE | DOI: 10.1109/ISCTRKIYE68593.2025.11224857

***Abstract*—Mobile cloud computing (MCC) improves performance and scalability by offloading tasks from mobile devices to cloud and edge infrastructure. Still, it remains vulnerable to low-speed denial-of-service (LDoS) and distributed denial-of-service (DDoS) attacks. This paper compares centralized, distributed, and hybrid architectures and evaluates their effectiveness using key metrics, including detection accuracy, latency, privacy, scalability, and deployment feasibility. In addition to comparing five representative models based on literature reviews, we conduct experimental evaluations of federated learning-based hybrid models using a recent Internet of Things (IoT) network traffic dataset that reflects modern attack patterns. The results indicate that while centralized models achieve the highest detection accuracy, they suffer from increased latency and reduced privacy; decentralized models improve response speed and privacy but face coordination challenges. Hybrid methods, especially those using federated learning, provide a well-rounded solution by offering strong security, flexibility, and efficient performance, making them ideal for practical use in MCC environments.**

Keywords—Mobile Cloud Computing, DDoS Detection, Federated Learning, Anomaly Detection, Hybrid Architecture, IoT Security

I. Introduction

As cloud computing becomes the foundation of the global digital infrastructure, security threats against cloud systems are escalating rapidly. According to a recent systematic review, cloud-related data breaches have increased from 1,200 in 2020 to more than 1,800 in 2023, a 50 percent increase in just three years [1]. Fig. 1 shows the year-over-year growth of cloud vulnerabilities, highlighting the increasing vulnerability of cloud systems, especially as mobile, Internet of Things (IoT), and edge devices continue to proliferate in the networked environment. It is projected that by 2034, there will be more than 40 billion IoT devices deployed globally, with consumer applications accounting for nearly 60 percent of that number [2]. Expanding endpoint diversity requires not only improved security protocols, but also an adaptable cloud architecture that can meet the latency and scalability requirements of real-time applications [3]. Traditional centralized cloud architectures, originally designed to deliver static web content, are becoming increasingly inadequate to handle modern data generation patterns.

In contrast to previous methods where users simply consumed material from faraway cloud servers, today's networks generate massive amounts of data at the edge. Sources of this data include industrial IoT platforms, autonomous systems, smart devices, and mobile applications. As technology and data volumes grow, edge computing has become an even more critical architectural concept. Instead of relying exclusively on centralized data centers, edge computing processes data close to the data source, which can significantly improve system efficiency while reducing latency and bandwidth consumption. More importantly, it provides an ingenious and valuable solution to the problems posed by modern decentralized data transfer methods, ultimately improving performance and security [4]. Relying on centralized data centers (often hundreds of kilometers away from the data source) can lead to severe delays in data transmission, overuse of network capacity, and a higher chance of failure due to the reliance on a single core system [5]. As a result, the vast potential of edge devices remains underutilized, as traditional centralized models typically ignore the growing processing power of edge devices [6]. The continued reliance on reliable cloud connectivity in IoT-driven environments reduces overall system efficiency and increases the risk of critical infrastructure compromise. In addition, it increases the risk of reliability issues if network connections are compromised or misused [7].

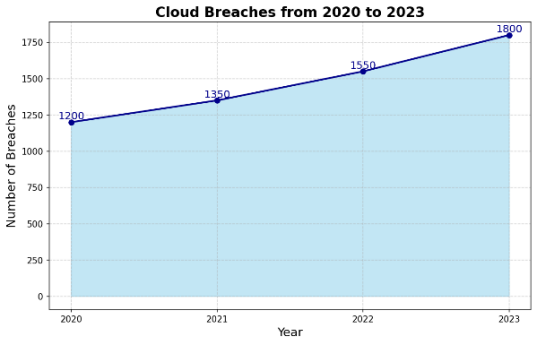

Fig. 1 Trend of cloud data breaches (2020–2023)

These architectural flaws directly impact cloud security. These limitations are particularly evident in distributed denial-of-service (DDoS) and low-rate denial-of-service (LDoS) attacks. Among DDoS threats, in addition to massive packet flooding, low-rate stealth attacks that disrupt quality of service and avoid detection are becoming more prevalent [8]. In mobile cloud computing (MCC) and cloud-edge

systems, which rely on distributed coordination, these attacks pose a serious threat to availability, scalability, and user trust.

Given the architectural weaknesses of traditional cloud systems in the face of these attacks, the adoption of alternative models such as decentralized and federated architectures has gained prominence. This paper addresses the growing need for secure, scalable, and privacy-aware architectures by analyzing and comparing three cloud security models: centralized, decentralized, and hybrid, in the context of DDoS detection. It also explores the role of federated learning as a privacy-preserving mechanism and highlights the potential of integrating blockchain technologies for decentralized trust and coordination:

- A comparative review of representative DDoS detection architectures in cloud and edge environments, selected based on architectural diversity, literature relevance, and availability of evaluation data.
- A comprehensive evaluation framework incorporating five core metrics: detection accuracy, latency, scalability, privacy, and deployment feasibility.
- Using a new IoT network traffic dataset, experimental validation of a federated learning-based hybrid model against DDoS attacks

The remainder of this paper is organized as follows. Section II provides background and reviews related work, including the selection criteria for five representative DDoS detection models. Section III presents the centralized, decentralized, and hybrid cloud–edge architectures, detailing their design principles, strengths, and limitations. Section IV introduces the evaluation framework and metrics used for the comparative study. Section V describes the experimental validation of the proposed federated learning–based hybrid model and reports its performance results. Section VI offers a comparative analysis and discussion of all models. Finally, Section VII concludes the study and outlines future research directions for adaptive, secure, and scalable MCC deployments.

II. Related Work

The evolution of MCC and distributed cloud–edge systems has spurred the development of various DDoS detection architectures that balance detection accuracy, latency, privacy, and scalability. Usually, these architectures can be divided into three groups: hybrid, decentralized, and centralized. A range of methods in line with these paradigms is presented in recent literature.

We have carefully selected five representative models-FlowGuard, RTVD, FR-RED, SoftEdgeNet, and FOGshield-from the existing literature to provide a comprehensive overview of the latest advances in DDoS detection in mobile cloud computing (MCC) and Internet of Things (IoT) environments. To ensure relevance and diversity, the selection process was based on the following criteria: (1) the latest publications that directly address mobile cloud computing and IoT security issues; (2) cover a range of architectural paradigms such as centralized, decentralized, and hybrid frameworks; (3) are published in respectable peer-reviewed journals or conferences; and (4) provide a comprehensive performance evaluation, especially in terms of accuracy and latency metrics. In summary, these models cover a wide range of modern approaches that are frequently cited or used in cloud edge security and distributed denial-of-service (DDoS) mitigation research.

FlowGuard represents a centralized approach, deploying deep learning (DL) models specifically convolutional neural network (CNN) and long short-term memory (LSTM) at edge gateways to detect IoT-based DDoS traffic with high accuracy (99.9% for CNN, 98.9% for LSTM). While it excels in real-time detection, its dependency on centralized computation introduces significant latency and requires high-performance edge infrastructure [9].

In contrast, decentralized models like real-time volumetric detection (RTVD) [10] and fractal residual based real-time detection of the LDoS attack (FR-RED) [11] emphasize statistical methods suitable for resource-constrained environments. RTVD combines quintile deviation measurements with entropy-based volumetric filtering to quickly identify flooding patterns. To detect hidden LDoS traffic with low false alarm rates, FR-RED employs fractal residual analysis and Hurst exponent computation. While these architectures provide distributed execution, coordination, and consistency of edge nodes can be problematic. SoftEdgeNet is a decentralized, non-ML based architecture that uses software-defined networking (SDN) to implement dynamic access control lists (ACLs) at the fog nodes. It improves scalability and energy efficiency while remaining decentralized by leveraging blockchain for rule integrity. Although it lacks adaptive learning capabilities, it works well for large-scale DDoS filtering [12].

Hybrid approaches aim to combine the strengths of centralized oversight with localized responsiveness. FOGshield utilizes federated learning to enable local training of self-organizing maps (SOMs) on fog nodes, with periodic centralized aggregation. This design preserves data privacy, reduces communication overhead, and maintains global model accuracy, making it well-suited for dynamic, privacy-sensitive environments [13]. Additional innovations in hybrid cloud–edge architectures include blockchain-augmented security and microservice-based hybrid edge cloud (HEC) models. For example, Khashan and Khafajah [14] proposed a blockchain-enhanced hybrid framework for DDoS mitigation, while Alamouti et al. [5] introduced HEC, a fully decentralized platform enabling service offloading across smart devices. Albshaier et al. [1] further confirmed the viability of federated learning in cloud-edge networks through a systematic review highlighting its effectiveness in threat detection and privacy preservation.

Collectively, these studies illustrate the ongoing trade-offs among architectural paradigms in DDoS defense highlighting the need for scalable, privacy-aware, and low-latency solutions in MCC and edge-enabled systems.

III. Cloud–Edge Security Architectures

A. Centralized Architecture

The simplicity and ease of engineering of centralized architectures have led to their widespread adoption. These models simplify conceptual and operational management by considerably reducing data redundancy and synchronization

problems. A typical example is the client-server model, which, as shown in Fig. 2 [15], involves multiple client devices interacting directly with a central cloud server for data processing and decision-making. In centralized systems, all data processing and analysis takes place on a remote cloud server. This architecture inherently has significant disadvantages, despite its advantages in terms of processing power, simplified control, and simplified policy administration. These include the higher risks associated with a single point of failure and the increased latency due to data transmission over long distances [16]. Additionally, sending data to centralized cloud servers from hundreds of billions of client devices can result in significant bottlenecks, wasting bandwidth and energy, and having major social and economic repercussions for large-scale deployments [5].

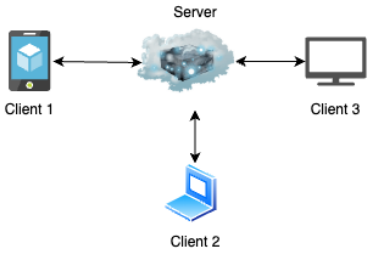

Fig. 2 Centralized cloud architecture

B. *Decentralized Architecture*

Decentralized architectures distribute computing and storage resources across multiple edge nodes and do not rely solely on a central cloud server for data processing and decision-making, as illustrated in Fig. 3. This design minimizes reliance on any central cloud server for core operations, thereby enhancing system resilience, reducing latency, and alleviating bandwidth congestion by removing single points of failure [17].

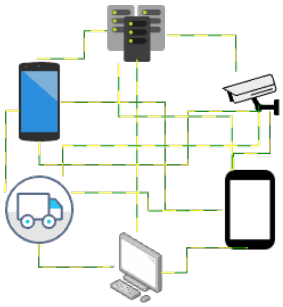

Fig. 3 Decentralized cloud architecture

However, some decentralized systems may interact with centralized cloud servers for helpful functions such as long-term data storage, advanced analytics, or backup purposes. Despite this occasional involvement of centralized components, the essential processing and security tasks are carried out in a distributed, peer-to-peer manner among edge nodes, preserving the benefits of decentralization[17]. Decentralization offers numerous advantages, but it also brings new challenges, especially regarding reliability and security. In networks where devices must remain online and responsive, targeted DDoS attacks can be extremely damaging. Such attacks, which may target specific devices or critical access points such as gateways, have the potential to disrupt or interrupt the flow of critical data. For example, if a smartphone loses connectivity due to a cyberattack or user outage during a live video stream, downstream communications may not work properly. This type of vulnerability highlights the need to have always available and reliable nodes (e.g., home routers or enterprise servers at the edge) [5].

C. *Hybrid Architecture*

Hybrid cloud design combines the benefits of both centralized and decentralized approaches, balancing security, scalability, and performance by mixing fog and edge computing resources [18]. This approach processes time-sensitive data locally on edge or fog nodes to minimize latency and enhance responsiveness, while delegating more complex, resource-intensive tasks such as comprehensive analytics, global model aggregation, or long-term data storage to centralized cloud servers.

FogShield's fusion of advanced cybersecurity features with fog computing concepts is an excellent example of this strategy in action. FogShield demonstrates how distributed and centralized resources can work together to address evolving cyber threats using a layered architecture concept. By connecting decentralized edge nodes to the main system, its intelligent, behavior-driven detection engine can quickly identify and obstruct widespread DDoS attacks. This hybrid decision-making system helps to detect threats early and improves network performance by reducing latency and conserving bandwidth [13]. Through hierarchical coordination and distributed learning of attack behaviors, this system demonstrates how hybrid models can provide reliable, real-time security for IoT networks [13]. As shown in Fig. 4, the hybrid architecture utilizes edge and cloud resources to improve response time and ensure network continuity in various scenarios.

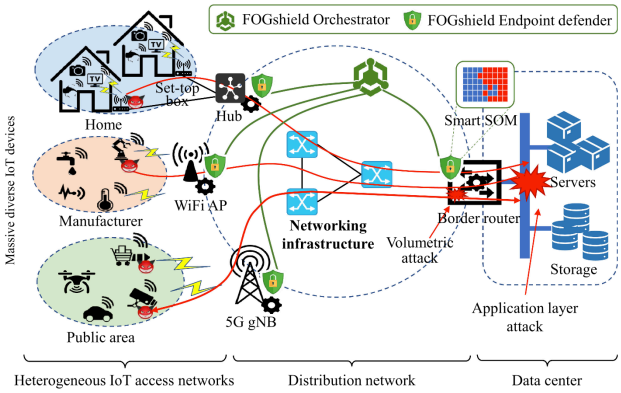

Fig. 4 Hybrid cloud architecture (FOGshield) [13]

IV. Comparison of Studies and Evaluation Metrics

This study uses several criteria to perform comparative analysis:

Accuracy: Shows the percentage of malicious activity that was correctly detected (true positives) out of all the evaluated instances. More accurate detection results in fewer false positives or negatives, which is essential for dependable defense systems.

Latency: Calculates the amount of time it takes for a system to react or take mitigation measures after an attack has begun. In real-time security scenarios, such as DDoS or LDoS

detection, reducing latency is critical to minimizing damage and avoiding service disruptions.

Scalability: Demonstrates how the system performs in areas such as detection accuracy as the number of users, devices, or traffic increases. a variety of large systems such as MCC networks and the Internet of Things are best suited for highly scalable solutions.

Privacy: This metric considers the system's ability to protect sensitive user or device data while performing threat detection. Federated learning or device analytics typically provide stronger privacy guarantees and pre-process data locally rather than sending raw data to a centralized server. Since gadgets store personal data, these technologies not only reduce the likelihood of leakage, but also enhance compliance with privacy regulations.

Deployment Feasibility: This metric measures how easy it is to integrate the detection solution with the current technology environment. It takes into account hardware dependencies, compatibility with existing software ecosystems, and deployment complexity. It is known that solutions that are lightweight, resource-efficient, and require minimal or no changes to existing infrastructure are more likely to be widely adopted.

Energy/Resource Usage: The standard allows a system's energy and processing power requirements to be assessed. This is particularly important in resource-limited environments, such as battery-powered mobile devices or IoT networks. Technologies with lower energy consumption and processing power are better suited to these environments. This efficacy not only extends the device's life but also supports broader goals.

Communication Overhead: This criterion measures the amount and regularity of data transfers between edge devices and central cloud servers or between decentralized nodes (e.g., edge-to-edge communication). In situations where network bandwidth is scarce or low latency is critical, technologies that require a small amount of communication tend to be more applicable. Reducing the frequency of data transmission can improve real-time responsiveness and system efficiency.

Based on published experimental results or technical descriptions in the literature, we evaluated each of the selected approaches and categorized them as centralized, decentralized, or hybrid based on their architectural model. Section VI, which presents this comparative analysis, details the tradeoffs of these architectures in terms of protecting the MCC and IoT ecosystems.

V. Experimental Validation: Federated Learning for DDoS Detection

This experiment uses the recently released CIC-BCCC-NRC ACI-IoT-2023 dataset [19] to evaluate the effectiveness of federated learning (FL) in detecting distributed denial-of-service (DDoS) attacks in IoT networks. The dataset records real IoT network traffic in benign and malicious environments, including various DDoS attack variants. Our objective is to determine whether FL can detect imbalanced network traffic in the real world with high accuracy while preserving the original data at local nodes.

A. Dataset and Preprocessing

The Canadian Institute for Cybersecurity (CIC) has released the TabularIoTAttack-2024 dataset [19], which includes the CIC-BCCC-NRC ACI-IoT-2023 dataset. In this study, only traffic related to DDoS attacks and benign network traffic were selected from all available traffic categories. This includes files such as Benign Traffic.csv, DoS DNS Flood.csv, DoS ICMP Flood.csv, DoS SYN Flood.csv, and DoS UDP Flood.csv. These network traffic data were collected in a controlled IoT laboratory environment to capture current and realistic IoT attack patterns.

Before training the model, a recursive feature elimination (RFE) [20] method based on logistic regression was used to select the 15 most important features for the classification task. This operation reduced the size of the dataset, improved training speed, and helped prevent overfitting. During the training phase, the SMOTE algorithm [21] was used to balance the feature-reduced dataset to ensure an even distribution of benign samples and DDoS samples in each client node. During the validation phase, the original unbalanced dataset was retained to simulate real-world scenarios with lower attack frequencies than normal traffic levels.

B. Federated Learning Setup

The experiment was conducted in a systematic manner. First, the training dataset was divided into three equal subsets, each of which was assigned to an independent client (or edge node). The SMOTE algorithm was used to balance the data within each client, ensuring that each client contained the same number of DDoS attack samples and normal samples. No raw traffic data was exchanged between the clients and the server; this balancing operation was performed locally on each client.

Subsequently, each client trained a logistic regression model using the balanced dataset. After training, the master node integrated the model parameters from each client using a weighted average to generate an updated global model. To reflect actual network traffic conditions, the global model was tested using the original unbalanced dataset.

C. Experimental Results

The FL model was evaluated on the CIC-BCCC-NRC ACI-IoT-2023 dataset using an imbalanced test set to reflect real-world network traffic. The model achieved an accuracy rate of 91% in normal traffic detection, with a precision rate of 93.06%, a recall rate of 95.49% and 94.26% F1 score. Fig. *5* illustrates the overall accuracy performance, highlighting the model's effectiveness in distinguishing DDoS attack traffic from regular traffic in a distributed learning environment.

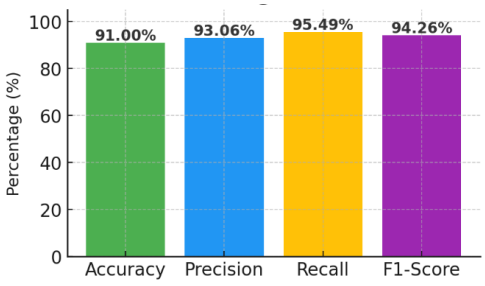

Fig. 5 FL model performance metrics of the experiment

We plotted a receiver operating characteristic (ROC) curve (as shown in *Fig. 6*) to further evaluate the classification capability of the proposed federated learning model. The model achieved an area under the curve (AUC) of 0.84, indicating its strong discriminatory power in distinguishing DDoS attacks from benign traffic. In real-world IoT environments, false positives may overwhelm monitoring systems. The steep initial rise of the curve indicates that the model maintains a high true positive rate while keeping the false positive rate at a relatively low level.

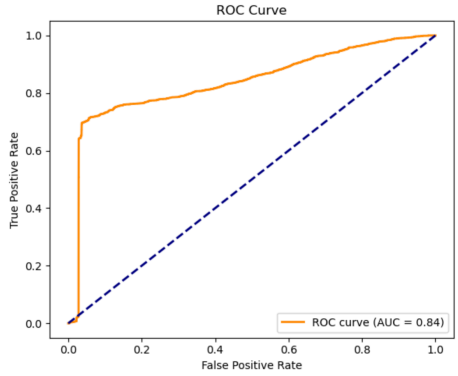

Fig. 6 ROC curve of the experiment

Batch prediction of 21,345 samples was completed in 12.3 milliseconds (approximately 1,735 samples/second throughput), while client training time was less than 0.45 seconds for any node. CPU utilization during training averaged approximately 12%, peaking at 84% during the probability estimation phase, with memory usage remaining below 46 MB at all times.

VI. Discussion

When comparing DDoS detection models under different cloud architectures, there is a clear trade-off between accuracy, privacy, latency, and deployment feasibility. TABLE 1 summarizes the technical characteristics of the five models, including their architecture types, learning strategies, communication structures, latency, and energy consumption requirements. Between centralized, distributed, and hybrid designs, these advantages and disadvantages must be carefully weighed to meet the requirements of the target operating environment.

Centralized models, such as FlowGuard [9], deliver very high accuracy through deep learning and cloud computing power, but incur higher latency, significant CPU usage (20–80%), and low privacy due to centralized data transfer. [9]. This level of resource usage confirms the model's classification as high energy/resource consumption. In addition, these systems typically offer low privacy protection because the raw data must be sent to a central server for analysis, which can create compliance and trust issues for sensitive applications. Decentralized approaches such as RTVD [10], FR-RED [11], and SoftEdgeNet [12] prioritize local data, resulting in low latency and high privacy key advantages for mobile and IoT environments. Among them, RTVD uses entropy-based detection with the QuinDC algorithm, achieving a detection delay of 15.2 ms and a false omission rate of 0.3448%. While its accuracy is rated moderate due to a lack of learning-based adaptation, RTVD provides moderate latency, low false positives, and efficient CPU usage, making it practical for real-time IoT settings. FR-RED [11] detects LDoS attacks using fractal residuals with the Hurst exponent, achieving 97.75% accuracy, low latency via a sliding window, and entirely local processing, with minimal computational cost.

TABLE 1 Comparative Evaluation of DDoS Detection Models Across Cloud Architecture Types

Model	Architecture Type	Privacy	Latency	Accuracy Performance	Energy/ Resource Usage	Learning Type	E2E Comm.	Cloud Comm.
FlowGuard	Centralized	Low	CNN ~1ms LSTM 4-47ms	High %99.9	High (Heavy DL model) 20–80% CPU	Supervised DL	❌	✅
RTVD	Decentralized	High	15.2 ms	Moderate (no reported %, based on statistical)	Low (rule based, fog & edge environment)	Statistical	❌	❌
FR-RED	Decentralized	High	Not reported (estimated low due to local statistical processing and no DL)	%97.75	Low (lightweight residual calculation)	Statistical	❌	❌
FOGshield	Hybrid (Federated)	High	Not reported (estimated low due to local federated fog-based processing)	High (Federated SOM) %99.5	Moderate %36 CPU	Federated Unsupervised	✅ (via server)	✅
SoftEdgeNet	Decentralized (Collaborative)	High	Not reported (response time analysis and edge-level processing indicate low latency without DL overhead)	Moderate (no reported %, based on heuristic ACL logic)	Very Low (reduced data logging and bandwidth usage)	Heuristic / Rule-based	✅ (via blockchain)	❌
Our FL-DDOS Model	Hybrid (Federated)	High	12.3 ms (batch)	Accuracy 91%,	Moderate (avg. 12% CPU, peak 84% during inference, ≤46 MB memory, no GPU)	Supervised	✅	✅ (via aggregation server)

Note: E2E Comm. = Edge-to-Edge Communication; Cloud Comm. = Cloud Communication; ✅ = Present, ❌ = Not present.

SoftEdgeNet [12], a blockchain-coordinated SDN architecture, sustains >6000 PPS in software, >9 Mbps in hardware, and 2000 PPS under saturation, offering low latency, high efficiency, and scalability, though accuracy is unspecified. FogShield [13] uses a hybrid joint unsupervised learning (SOM) approach where fog nodes detect anomalies locally and share only model updates, ensuring privacy. By processing data on-site, it achieves low latency, and its continuous local learning enables adaptivity to changing traffic patterns without central retraining. This design delivers high accuracy with moderate energy use, making it ideal for resource-limited fog environments. The FL-based hybrid model we propose adopts this balanced approach by training a distributed logistic regression model using the CIC-BCCC-NRC ACI-IoT-2023 dataset and aggregating it on a central server. The model achieves 91% accuracy, 93.06% precision, 95.49% recall, and 94.26% F1 score, with batch inference latency of 12.3 milliseconds and moderate resource consumption (average 12% CPU, additional memory $\leqslant$46 MB). Although its accuracy is slightly lower than that of top-tier centralized deep learning methods, the model offers significant advantages in terms of privacy protection, bandwidth requirements, and efficient, scalable detection on distributed IoT nodes, benefits that cannot be achieved in a fully centralized architecture.

VII. Conclusion and Future Work

This study compares centralized, distributed, and hybrid architectures for distributed denial-of-service (DDoS) detection in cloud edge environments, focusing on the trade-offs between accuracy, latency, privacy, and resource utilization. While centralized models achieve the highest accuracy, they suffer from high latency and low privacy. Distributed designs, though capable of providing fast and privacy-preserving detection, come at the cost of increased coordination complexity. Hybrid approaches, such as FogShield and the proposed FL-based model, achieve a balance between high accuracy, low latency, and strong privacy protection through distributed learning and selective aggregation. Future research should focus on building an adaptive framework that can dynamically switch architectures based on network conditions, integrating blockchain, zero trust, and federated learning technologies, and verifying its performance in large-scale real IoT deployment environments.

References

[1] Albshaier, L., S. Almarri, and A. Albuali, *"Federated Learning for Cloud and Edge Security: A Systematic Review of Challenges and AI Opportunities,"* Electronics (Switzerland), vol. 14, no. 5, p. 1019, Mar. 2025, doi: 10.3390/ELECTRONICS14051019/S1.

[2] Vailshery, L. S., "IoT connections worldwide 2034| Statista," Statista. Accessed: May 27, 2025. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[3] Shukla, S., M. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan, and M. K. Khan, *"Improving latency in Internet-of-Things and cloud computing for real-time data transmission: a systematic literature review (SLR),"* Cluster Computing, vol. 26, no. 5, pp. 2657–2680, Oct. 2023, doi: 10.1007/S10586-021-03279-3/TABLES/14.

[4] Ghazwan Khalid, H., H. Hadi Abbas, M. Jabbar Hussein, M. Jawad Abu-AlShaeer, S. Khdhaer Mukhlif, and D. Khlaponin, *"Unveiling the Next Frontier: The Future of Connected Technologies,"* in *Conference of Open Innovation Association, FRUCT*, 2024. doi: 10.23919/FRUCT64283.2024.10749851.

[5] Alamouti, S. M., F. Arjomandi, and M. Burger, *"Hybrid Edge Cloud: A Pragmatic Approach for Decentralized Cloud Computing,"* IEEE Communications Magazine, vol. 60, no. 9, pp. 16–29, Sep. 2022, doi: 10.1109/MCOM.001.2200251.

[6] Trajano, A. F. R. and J. N. de Souza, *"Harnessing idle edge resources for execution of cloud services: A comprehensive review,"* Transactions on Emerging Telecommunications Technologies, vol. 35, no. 4, p. e4966, Apr. 2024, doi: 10.1002/ETT.4966.

[7] Escamilla-Ambrosio, P. J., A. Rodríguez-Mota, E. Aguirre-Anaya, R. Acosta-Bermejo, and M. Salinas-Rosales, "Distributing computing in the internet of things: Cloud, fog and edge computing overview," in *Studies in Computational Intelligence*, vol. 731, Springer Verlag, 2018, pp. 87–115. doi: 10.1007/978-3-319-64063-1_4/FIGURES/17.

[8] Uddin, R., S. A. P. Kumar, and V. Chamola, *"Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions,"* Ad Hoc Networks, vol. 152, p. 103322, Jan. 2024, doi: 10.1016/J.ADHOC.2023.103322.

[9] Jia, Y., F. Zhong, A. Alrawais, B. Gong, and X. Cheng, *"FlowGuard: An Intelligent Edge Defense Mechanism against IoT DDoS Attacks,"* IEEE Internet of Things Journal, vol. 7, no. 10, pp. 9552–9562, Oct. 2020, doi: 10.1109/JIOT.2020.2993782.

[10] Li, J., M. Liu, Z. Xue, X. Fan, and X. He, *"Rtvd: A real-time volumetric detection scheme for ddos in the internet of things,"* IEEE Access, vol. 8, pp. 36191–36201, 2020, doi: 10.1109/ACCESS.2020.2974293.

[11] Tang, D., Y. Feng, S. Zhang, and Z. Qin, *"FR-RED: Fractal Residual Based Real-Time Detection of the LDoS Attack,"* IEEE Transactions on Reliability, vol. 70, no. 3, pp. 1143–1157, Sep. 2021, doi: 10.1109/TR.2020.3023257.

[12] Sharma, P. K., S. Rathore, Y. S. Jeong, and J. H. Park, *"SoftEdgeNet: SDN Based Energy-Efficient Distributed Network Architecture for Edge Computing,"* IEEE Communications Magazine, vol. 56, no. 12, pp. 104–111, Dec. 2018, doi: 10.1109/MCOM.2018.1700822.

[13] Dao, N. N. *et al.*, *"Securing Heterogeneous IoT With Intelligent DDoS Attack Behavior Learning,"* IEEE Systems Journal, vol. 16, no. 2, pp. 1974–1983, Jun. 2022, doi: 10.1109/JSYST.2021.3084199.

[14] Khashan, O. A. and N. M. Khafajah, *"Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems,"* Journal of King Saud University - Computer and Information Sciences, vol. 35, no. 2, pp. 726–739, Feb. 2023, doi: 10.1016/J.JKSUCI.2023.01.011.

[15] Kratzke, N., *"A Brief History of Cloud Application Architectures,"* Applied Sciences 2018, Vol. 8, Page 1368, vol. 8, no. 8, pp. 1368, Aug. 2018, doi: 10.3390/APP8081368.

[16] Gao, J., H. Wang, and H. Shen, *"Task Failure Prediction in Cloud Data Centers Using Deep Learning,"* IEEE Transactions on Services Computing, vol. 15, no. 3, pp. 1411–1422, 2022, doi: 10.1109/TSC.2020.2993728.

[17] Sasikumar, A. *et al.*, *"A Decentralized Resource Allocation in Edge Computing for Secure IoT Environments,"* IEEE Access, vol. 11, pp. 117177–117189, 2023, doi: 10.1109/ACCESS.2023.3325056.

[18] Gundu, S. R., C. A. Panem, and A. Thimmapuram, *"Hybrid IT and Multi Cloud an Emerging Trend and Improved Performance in Cloud Computing,"* SN Computer Science, vol. 1, no. 5, pp. 1–6, Sep. 2020, doi: 10.1007/S42979-020-00277-X/FIGURES/2.

[19] "Tabular IoT Attack 2024 | Datasets | Research | Canadian Institute for Cybersecurity | UNB." Accessed: Aug. 08, 2025. [Online]. Available: https://www.unb.ca/cic/datasets/tabular-iot-attack-2024.html

[20] Ramírez-Hernández, J. A. and E. Fernandez, *"Control of a re-entrant line manufacturing model with a reinforcement learning approach,"* Proceedings - 6th International Conference on Machine Learning and Applications, ICMLA 2007, pp. 330–335, 2007, doi: 10.1109/ICMLA.2007.35.

[21] Chawla, N. V., K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, *"SMOTE: Synthetic Minority Over-sampling Technique,"* Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, Jun. 2002, doi: 10.1613/JAIR.953.