International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

MCCS: PRIVACY-ENHANCED AND ADVERSARIAL-RESILIENT MULTI-CRITERIA CLIENT SELECTION FOR FEDERATED LEARNING IN IOV

Jadil Alsamiri[1]*, Khalid Alsubhi[2]
[1]*Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; jalsamiri@stu.kau.edu.sa
[2]Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia; kalsubhi@kau.edu.sa
***Corresponding Author:** Jadil Alsamiri
*jalsamiri@kau.edu.sa)

Abstract:
The Internet of Vehicles (IoV) generates extensive data for machine learning applications such as intrusion detection; however, centralized solutions often create privacy and security risks. Federated Learning (FL) enables decentralized training while ensuring that data remain local. However, in IoV contexts, it is challenged by client heterogeneity, non-independent and identically distributed data, and adversarial attacks. This study, therefore, proposes a Multi-Criteria Client Selection (MCCS) framework that selects clients based on trust, connectivity, data diversity, and adversarial behavior for secure and robust FL operation. Key innovations are a dynamic trust-score mechanism with cosine similarity against adversaries, a combination of data diversity with improved generalization, differential privacy for a balance between privacy and performance, and scalability for constrained devices. Evaluated with simulations over the Car Hacking dataset, MCCS demonstrated strong results with F1 scores of 0.7590 to 0.8678, a maximum accuracy of 0.9775, convergence between 510 and 1459 seconds, and memory use of 1,964 to 3,137 MB, outperforming baselines such as FedPROM and RICA+CKA.

Keywords: Federated Learning; Internet of Vehicles (IoV); Multi-Criteria Client Selection (MCCS); Intrusion Detection; Adversarial Resilience; Differential Privacy.

1. Introduction

1.1 Background and Motivation

The Internet of Vehicles (IoV) is a new development in automotive technology, where vehicles, sensors, and infrastructure are connected together to build smart transport systems designed to improve safety, ease traffic, and give users personalized services through real-time vehicle-to-vehicle, vehicle-to-infrastructure, and vehicle-to-everything communication [1]. This shift has led to an exponential increase in data generation, encompassing vehicle diagnostics, driving behaviors, traffic patterns, and environmental conditions, which, when harnessed via machine learning, can accelerate innovations such as predictive maintenance, adaptive navigation, and autonomous driving capabilities [2]. For example, using large amounts of driving data to train models can make obstacle detection in self-driving cars more reliable and safer [3]. However, centralizing sensitive vehicular data poses serious concerns: privacy violations under the General Data Protection Regulation, elevated security threats from cyberattacks, and network overload from bandwidth limits [4]. To tackle these issues, this study examines client selection techniques in Federated Learning (FL). Research has shown that FL allows vehicles to keep data locally and send only model updates, which helps protect privacy,

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

reduces communication costs, and supports safer and more efficient transportation systems [5, 6, 45].1.2 Problem Statement

Despite the promise of FL in IoV, deployment is hindered by the dynamic and heterogeneous nature of vehicular networks [1, 3]. Vehicles vary in computational power, storage, and connectivity, leading to imbalanced training and slow convergence [1]. Rapid mobility reshapes IoV topologies, causing fluctuations in bandwidth, latency, and link stability that disrupt synchronization and communication [3]. Vehicular data are often non-IID, introducing bias and limiting model adaptability to diverse traffic scenarios [7]. Moreover, the openness of IoV networks exposes FL to poisoned or manipulated updates, threatening global model reliability [5, 41]. Traditional client selection strategies—random or resource-based—fail to address trust, data diversity, and adversarial risks, thereby undermining FL's security, efficiency, and scalability in IoV [8, 22]. To address these challenges, this study proposes a new client selection method to enhance FL's robustness and adaptability for IoV [9].

1.3 Research Objectives

The objective of this work is to design and evaluate a client selection framework for FL in IoV, focusing on security, privacy, and efficiency. The proposed Multi-Criteria Client Selection (MCCS) framework incorporates client trustworthiness and data diversity to improve model robustness and generalization. The study also examines the role of differential privacy (DP) in balancing data protection with intrusion detection accuracy and evaluates the framework's scalability and resilience against adversarial attacks.

1.4 Contributions

This work advances FL in IoV by introducing an MCCS that evaluates clients based on trust, connection reliability, data variability, and adversarial behavior to improve model efficiency and security. It leverages advanced data diversity metrics to better handle non-IID distributions, enhancing model generalizability across scenarios such as urban traffic and highways. A dynamic trust mechanism adjusts scores using model update similarities, enabling gradual detection and mitigation of adversarial clients. Integrating DP balances accuracy and privacy while supporting compliance and effective threat detection.

2. Related Work

2.1 Overview of Federated Learning in IoV

FL represents a pivotal innovation within IoV that facilitates decentralized model training across distributed vehicles while addressing fundamental challenges related to data privacy and communication efficiency in intelligent transportation networks [43]. This approach enables vehicles to train a shared global model collaboratively using their local information while preventing the transfer of raw data [50]. This design mitigates the risks of breaches and bandwidth overloads that influence centralized repositories in dynamic IoV networks [11]. This approach is most suitable for IoV, where it is required to handle vast amounts of heterogeneous data from vehicle sensors, such as traffic flows, vehicle diagnostics, and environmental conditions, that support applications such as predictive maintenance and anomaly detection [12].

Recent advancements have highlighted FL's capability of enhancing IoV security, such as through the use of intrusion detection based on edge computing that processes data locally, decreases latency, and enhances real-time responses to cyberattacks such as data poisoning or eavesdropping [13]. For

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

instance, FL frameworks incorporating blockchain have been proposed as solutions for secure aggregation of model updates, fostering trust and robustness in multi-vehicle environments [10, 14]. Further, asynchronous forms of FL have been studied so that IoV variability caused by mobility can be managed and vehicles can send updates at their own pace, thus increasing scalability under high-mobility scenarios [14]. Recent work also integrates FL with 6G-enabled networks for split learning that increases performance under low-resource situations [43, 49] and provides opportunities in vehicular networks [47].

However, although FL has great advantages, its application within IoV has inherent limitations, such as non-IID data distributions among vehicles, which may cause biased models and low generalization [15]. Because vehicular nodes are usually limited in processing power and have unstable connections, effective client selection procedures are needed to achieve a balanced participation and energy efficiency [16]. Overcoming these limitations requires higher-level approaches, such as MCCS, to boost the security and adaptability of FL within IoV [17]. Particularly, MCCS can advance the capacity of FL to secure IoV systems against threats [17].

2.2 Existing Client Selection Strategies

Client selection strategies in FL for IoV are instrumental in optimizing model efficiency, convergence rate, and resource utilization amid the unique challenges of vehicular networks, such as mobility-induced heterogeneity and security risks. These strategies generally fall into four categories: random-based, resource-based, stability-based, and multi-criteria. Each strategy tackles certain IoV dynamics while exposing shortcomings that our MCCS framework seeks to overcome. Random-based strategies grant all clients equal selection probabilities to foster fairness and inclusivity; however, they tend to perform poorly under conditions of network heterogeneity, where different vehicles have different hardware and data distributions, resulting in prolonged convergence and lower accuracy [18]. For example, modifications such as Fed-RHLP prioritize high-performing clients to boost convergence by up to 15%, yet they overlook adversarial risks and assume uniform resource availability, making them unsuitable for dynamic IoV settings [19]. Stochastic selections, while balancing inclusivity, incur security risks due to the absence of resources or trust awareness [20]. Resource-based strategies shift focus to vehicles with superior processing power, stable connectivity, and energy reserves to minimize dropouts in mobile IoV settings, achieving accuracy gains of up to 18% through clustering similar resource levels, as seen in FedCDRC [21]. However, these methods frequently neglect malicious clients and risk biasing the global model by excluding valuable but resource-constrained vehicles, particularly in mobility-aware selections that prioritize speed and location but ignore data diversity [22].

Stability-based methods further refine client selection by prioritizing reliable participants to mitigate erratic updates, with approaches such as RICA reporting a 125% improvement in accuracy against adversarial behaviors while concurrently reducing energy demands [21]. While they provide such advantages, they introduce computational complexities due to multi-objective optimizations and are biased against "less stable" but honest clients, constraining fairness at large scales of IoV deployment [23]. In contrast, MCCS employs a unified codebase that combines trust and diversity to offer superior robustness. Multi-criteria strategies adopt a holistic perspective that combines factors such as data quality, resources, and trustworthiness. This allows them to simultaneously address challenges like convergence speed and precision in frameworks such as FedPROM and FedAHP [24]. More advanced

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

methods, like RICA+CKA, use trust metrics for attack detection and security; however, they usually need more computation and do not scale well in IoV systems with limited resources [25]. Although they go beyond single-criterion methods, they often fail to protect privacy or handle non-IID data, highlighting the need for more adaptive solutions like MCCS. As shown in Table 1, MCCS outperforms existing methods by addressing IoV challenges comprehensively and achieving superior F1 scores and resilience.

Table 1: Comparison of Existing Client Selection Strategies in FL for IoV

Strategy Type	Example Methods	Year	Focus	Strengths	Limitations	Handles Adversarial Threats?	Supports Privacy?
Random-Based	Fed-RHLP [19]	2024	Equal probability, performance prioritization	Fairness, improved convergence (15%)	Overlooks adversaries, assumes uniform resources	No	Partial
Random-Based	FedNaWi [23]	2023	Weighted random selection	Speeds up training, prioritizes reliable clients	Lacks explicit adversarial mitigation, non-IID underexplored	No	Partial
Resource-Based	FedCDRC [21]	2024	Clustering by resource availability	Reduces dropouts, accuracy gains (18%)	Neglects malicious clients, may exclude valuable devices	No	No
Resource-Based	Mobility-Aware Selection [22]	2024	Selection based on speed/location	Minimizes disruptions, enhances training continuity	Lacks adversarial detection, biased if mobility is sole criterion	No	No
Stability-Based	RICA [21]	2024	Stability and malicious client detection	Accuracy boost (125%), minimizes dropout	Requires complex optimization, biased against "less stable" clients	Partial	No
Stability-Based	FedNaWi (stability variant) [23]	2023	Stability + energy efficiency	Achieves 55% energy reduction,	Not tailored for large-scale adversaries,	No	No

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Strategy Type	Example Methods	Year	Focus	Strengths	Limitations	Handles Adversarial Threats?	Supports Privacy?
				improves accuracy	overlaps with random		
Multi-Criteria	FedPROM, FedAHP [24]	2024	Resource, net conditions, multifactor selection	Improves convergence speed, enhances precision	Limited adversarial handling, complex tuning	No	Partial
Multi-Criteria	BiGE, GWO [26]	2024	Balanced resources, performance	Adapts to IoV conditions, minimizes inefficiencies	Heavy computation, lacks explicit security layer	No	No
Multi-Criteria	RICA+CKA [25]	2025	Adversarial detection and performance	Identifies malicious clients, emphasizes security	Higher overhead, biased against new clients	Yes	Partial
Proposed (MCCS)	MCCS	2025	Trust, diversity, adversarial penalties	Superior F1 scores (0.8678), privacy integration	N/A (addresses gaps)	Yes	Yes

2.3 Challenges and Limitations in Current Approaches

Substantial challenges and limitations in existing client selection strategies hinder the effectiveness of FL for IoV in dynamic and heterogeneous environments. A major challenge is client heterogeneity resulting from differences in computational resources, data distributions, and network conditions. These differences cause inconsistent updates and delayed convergence, as reported in many surveys [21]. For instance, random-based approaches such as Fed-RHLP struggle with non-IID data, resulting in biased global models that fail to generalize across diverse IoV scenarios, such as urban versus rural traffic patterns [27]. Resource-based strategies amplify the problem by favoring high-resource clients, which may exclude constrained but valuable participants and introduce unfairness [28]. Adversarial behaviors form another key limitation, as malicious clients can poison updates and compromise the IoV model's integrity. RICA uses reliability checks to address this, but it often fails in large deployments due to high costs and incomplete detection [29].

Another challenge is privacy protection in vehicular networks. Many strategies lack robust mechanisms like DP, leaving sensitive vehicular data vulnerable to inference attacks during aggregation [30]. Recent works on AI-powered Internet of Things emphasize cybersecurity in FL but

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

overlook integrated multi-criteria selection [42, 44]. Scalability remains a persistent hurdle, particularly in high-mobility IoV settings. Fluctuating connectivity causes dropouts and latency, restricting multi-criteria approaches that require complex optimization [31]. Moreover, current methods often fail to consider the interplay between challenges, such as balancing energy efficiency with adversarial resilience, leading to suboptimal performance in resource-scarce environments [32]. These challenges underscore the need for adaptive frameworks like MCCS. Table 2 compares selected approaches across strengths and weaknesses, positioning MCCS as a superior solution.

Table 2: Comparison of Selected Approaches in FL for IoV

Approach	Year	Strengths	Weaknesses	Comparison to MCCS
Stackelberg Game-Based FL [7]	2025	Optimizes incentives for participation, improves convergence in game-theoretic models	Lacks multi-criteria evaluation, overlooks trust and diversity, vulnerable to non-IID biases	MCCS integrates trust and diversity for enhanced resilience, outperforming in adversarial and heterogeneous scenarios
Fed-RHLP [19]	2024	Promotes fairness, boosts convergence by 15%	Assumes uniform resources, ignores adversaries	MCCS adds adversarial penalties and data diversity, achieving higher F1 scores (0.8678)
FedCDRC [21]	2024	Reduces dropouts, accuracy gains (18%)	Neglects malicious clients, biases toward resource-rich devices	MCCS balances resources with trust, mitigating biases and supporting privacy
RICA [21]	2024	Accuracy boost (125%), minimizes erratic updates	High complexity, potential bias against less stable clients	MCCS reduces overhead through dynamic criteria, improving scalability
BiGE, GWO [26]	2024	Adapts to IoV conditions, minimizes inefficiencies	Heavy computation, lacks explicit security layer	MCCS incorporates security and efficiency, with lower memory usage (1,964–3,137 MB)
Trust-Based Framework [32]	2024	Ensures high accuracy, low overhead	Focuses on trust but overlooks non-IID handling	MCCS combines trust with diversity, handling non-IID better (F1=0.7590)
Proposed (MCCS)	2025	Superior F1 scores (0.8678), privacy integration, handles non-IID, and adversaries	N/A (addresses gaps)	-

2.4 Comparison and Positioning of the Proposed Approach

While current client selection strategies focus on optimizing FL for IoV, they fail to address persistent challenges such as adversarial resilience, privacy preservation, and handling non-IID data

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

distributions [46], which our MCCS framework effectively mitigates by integrating multiple criteria, as shown in Table 3. For instance, game-theoretic approaches such as Stackelberg-based FL models are effective in incentivizing client participation through dynamic equilibrium. However, they often overlook multi-criteria evaluation [7] and focus primarily on resource allocation without integrating trust mechanisms or data diversity, leading to vulnerabilities in heterogeneous IoV environments [33]. In contrast, MCCS applies trust scoring alongside diversity metrics to reinforce resilience, providing more effective handling of non-IID data and achieving superior F1 scores of up to 0.8678 in simulated adversarial scenarios. Likewise, fairness-based methods prioritize equitable client engagement to minimize bias, yet they frequently compromise on efficiency in resource-scarce settings and lack robust defenses against poisoning attacks [34]. MCCS addresses this by ensuring balanced and secure model aggregation through incorporating adversarial penalties alongside privacy-aware criteria.

Other strategies, such as multi-armed bandit (MAB)-based selections, improve training latency in intelligent transportation systems but fail to handle dynamic threats or non-IID data effectively, resulting in suboptimal generalization across varying IoV conditions [22]. MCCS outperforms these by dynamically adapting to such heterogeneities through its holistic criteria, demonstrating convergence times of 510–1,459s with low memory usage. Trust-based frameworks further emphasize security in vehicular networks but often neglect scalability for large client counts, limiting their applicability in real-world IoV deployments [35]. By scaling efficiently up to 50 clients while maintaining high performance (F1=0.6794–0.8222), MCCS positions itself as a more comprehensive solution. Emerging works on blockchain-driven FL for anomaly detection in IoV highlight incentive mechanisms but still undervalue multi-level client criteria [17] and mobility-aware self-supervised learning [48]. These comparisons underscore MCCS's strengths in integrating privacy (via DP with ε=0.5–2.0), adversarial mitigation, and efficiency, filling critical gaps in current literature [36], as surveyed in FL for 6G networks [49].

Table 3: Comparison of MCCS with Selected Approaches in FL for IoV

Approach	Year	Focus	Strengths	Weaknesses	Comparison to MCCS
Stackelberg Game-Based FL [33]	2024	Dynamic incentives for participation	Optimizes equilibrium, improves convergence	Lacks multi-criteria, overlooks trust and diversity	MCCS integrates trust and diversity for better resilience, achieving higher F1 scores (0.8678)
FairEquityFL [34]	2025	Equitable opportunity for clients	Reduces selection bias, enhances fairness	Compromises efficiency, lacks adversarial defense	MCCS adds adversarial penalties, balancing fairness with superior privacy and performance
MAB-Based Selection [22]	2024	Latency reduction in ITS	Improves training efficiency, minimizes delays	Fails in non-IID data, vulnerable to threats	MCCS handles non-IID effectively (F1=0.7590), with

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Approach	Year	Focus	Strengths	Weaknesses	Comparison to MCCS
					faster convergence (510–1,459s)
Trust-Based Framework [35]	2025	Security-focused selection in IoV	Ensures high accuracy, low overhead	Limited scalability, neglects data diversity	MCCS scales to 50 clients while combining trust with diversity for enhanced generalization
Long-Term Client Selection [36]	2025	Handling non-IID over extended periods	Maximizes long-term welfare, adapts to skew	Overlooks privacy, high computational cost	MCCS incorporates DP (ε=0.5–2.0), outperforming in non-IID scenarios
Proposed (MCCS)	2025	Trust, diversity, adversarial penalties	Superior F1 scores (0.8678), privacy integration, handles non-IID, and adversaries	N/A (addresses gaps)	-

3. Proposed Methodology

The MCCS framework presented in this study enhances FL for securing IoV systems. It evaluates clients based on trustworthiness, connection quality, data diversity, and adversarial behavior, leading to stronger training and better handling of privacy, security, and heterogeneity issues. By integrating criteria dynamically, the framework selects optimal clients and adapts to network shifts, ensuring robust performance in threat-prone, data-rich IoV settings. This holistic design minimizes communication overhead, maximizes detection accuracy, and supports scalable deployment. It is particularly well-suited for IoV, where centralized data processing is limited by privacy regulations and bandwidth constraints [33].

3.1 Overview of the MCCS Framework

MCCS integrates centralized server-side coordination with client-side metric evaluation to enable effective selection and secure model aggregation. The main benefits of MCCS include better generalization via diversity, improved security against adversaries through trust penalties, preservation of privacy through optional differential privacy, and adaptability in constrained systems. For example, in IoV scenarios of high mobility, MCCS selectively prioritizes clients with stable connections and penalizes clients demonstrating suspicious update behaviors, thus maintaining the integrity of models without requiring full data sharing. This unified design reduces latency and energy consumption, critical for battery-limited vehicles, while fostering collaborative learning across distributed nodes.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

3.2 Key Components

Figure 1 depicts the high-level modular and interconnected architecture of the MCCS framework. The framework includes four fundamental components: trust evaluation, connection quality, data diversity, and adversarial penalty. These components combine into a composite score used for making seamless client selection. Each of the metrics serves a unique purpose so that a balanced and adaptive selection mechanism is guaranteed.

Trust measurement (Ti) employs cosine similarity between local and global model updates to assess reliability, thereby identifying trustworthy contributions and preventing adversarial behavior. For example, when model poisoning occurs, similarity scores fall. If Ti drops below the threshold, the system detects compromised clients and removes them. Connection quality (Ci) is determined using normalized latency and bandwidth values. This is especially useful in IoV, where mobility creates unstable connections. By prioritizing strong connections, MCCS mitigates failures and reduces latency [4].

Data diversity (Di) employs cosine similarity, with an emphasis on comparing data profiles, to ensure that the system learns from many types of data, not only repeating the same pattern. In IoV, this helps the model capture traffic patterns and avoid local bias [5]. Adversarial behavior penalty sets Ai=1.0 when Ti is below the threshold and decreases the selection probability. The penalty works cooperatively with trust evaluation to exclude suspicious clients in real-time and make the system more protected against data poisoning [6].

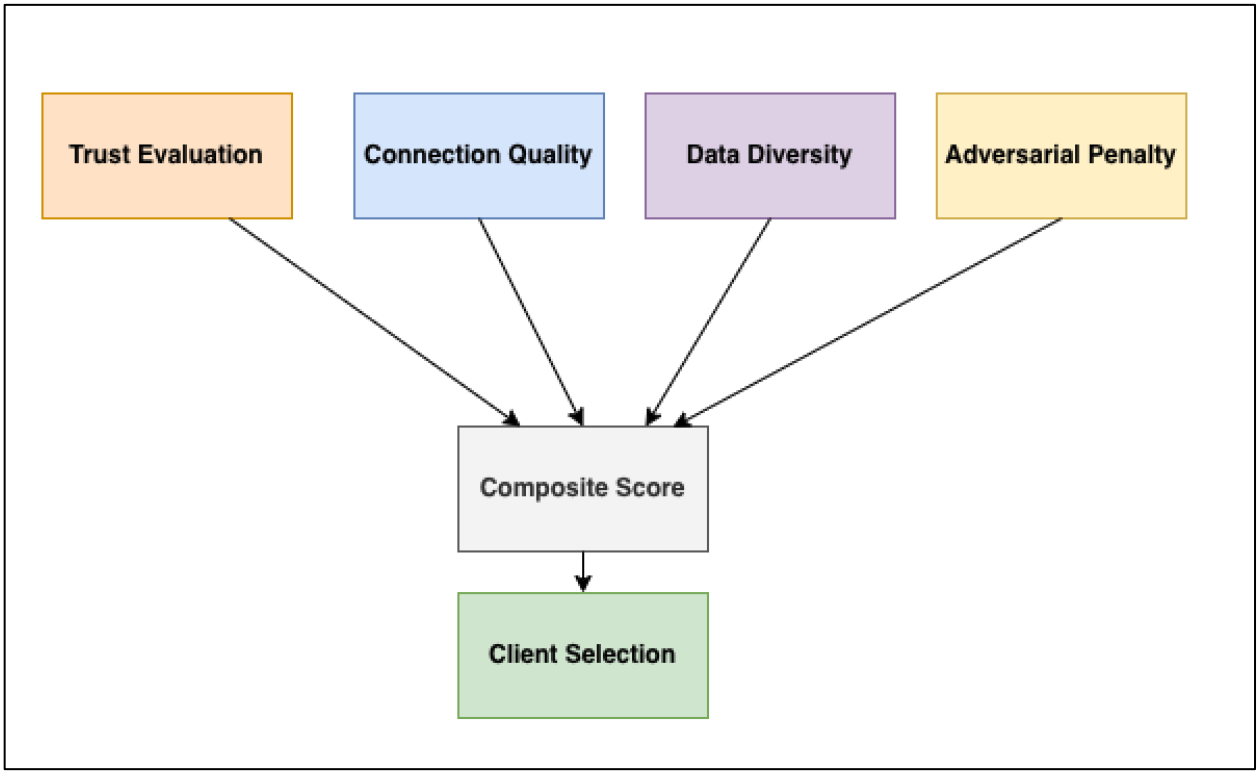


Figure 1: High-Level Architecture of MCCS Framework.

These components are weighted with tunable or dynamic weights, allowing them to adapt to environmental changes for better performance. Figure 2 illustrates trust score calculation, plotting cosine similarity against normalized update difference under a threshold. The graph shows a linear

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

relationship, with areas below the threshold (0.65) shaded in red to indicate low trust and penalty activation, while above-threshold areas are green for high trust. The figure explains how MCCS identifies reliable versus suspicious updates.

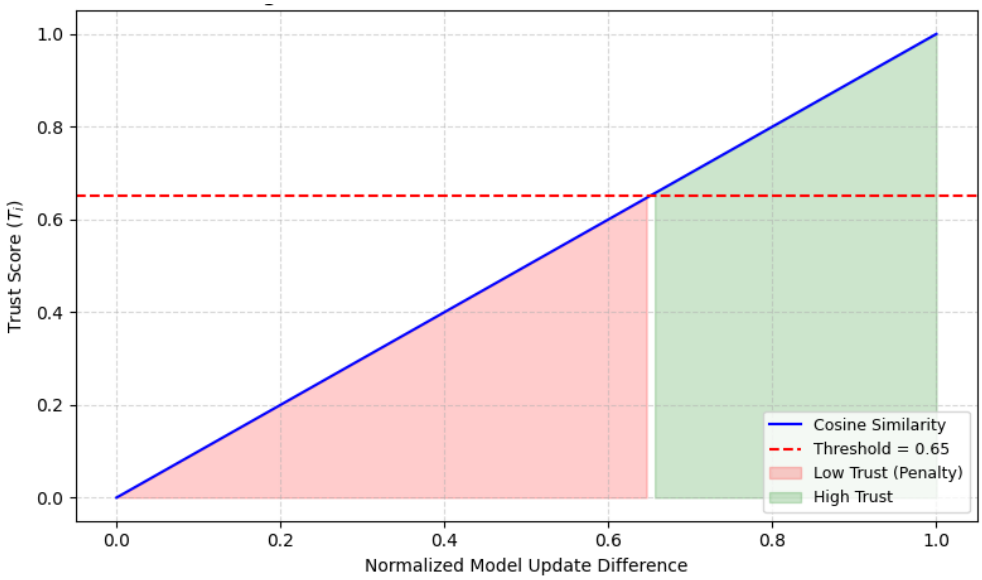


Figure 2: Example of Trust Score Calculation with Threshold.

3.3 Composite Scoring and Client Selection

The composite score *Si* integrates the components for prioritized selection, forming the core of MCCS's decision-making process. Formally, the composite score for client *i* is defined as:

$$S_i = w_t T_i + w_c C_i + w_d D_i - w_a A_i$$

where w_t, w_c, w_d, and w_a are tunable weights for trust, connection quality, data diversity, and adversarial penalty, respectively (for example, $w_t = 0.4$, $w_c = 0.2$, $w_d = 0.2$, $w_a = 0.2$). The values T_i, C_i, D_i, and A_i are normalized between 0 and 1.

The trust score T_i is computed using cosine similarity between the local model update vector u_i and the global model vector g.

$$T_i = \frac{u_i \cdot g}{|u_i|\,|g|}$$

If $T_i < \theta$ (threshold, e.g., 0.65), then $A_i = 1$ (penalty applied); otherwise, $A_i = 0$.

The connection quality *Ci* is normalized as:

$$C_i = \frac{b_i/l_i}{\max(b/l)}$$

where b_i is bandwidth and l_i is latency. Data diversity D_i uses cosine similarity of data feature vectors across clients.

Received: August 13, 2025

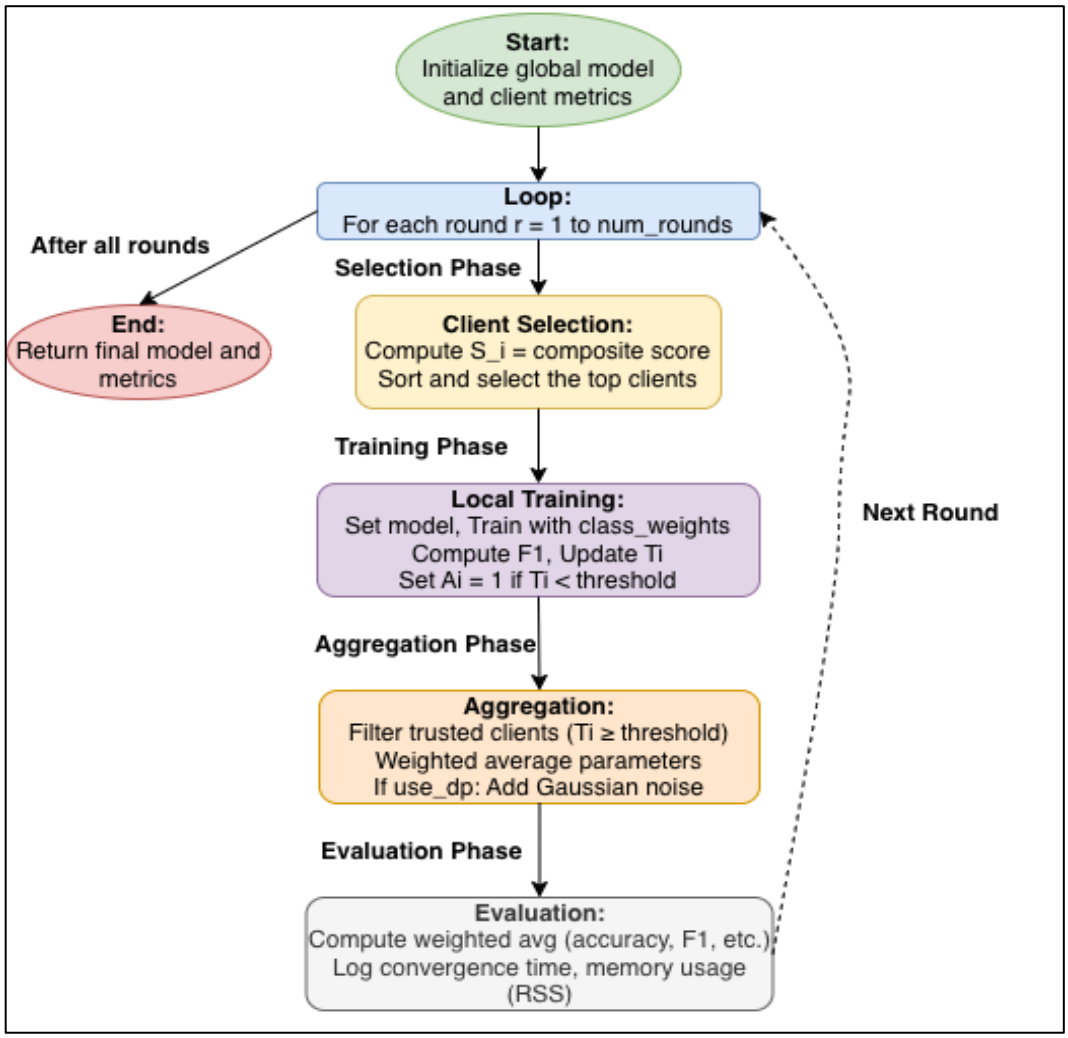
International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Clients are ranked by S_i, and the top group is selected, supporting flexible aggregation and DP noise for protection against inference attacks [13]. This scoring mechanism filters out unreliable participants. It also promotes balanced contributions, ensuring accuracy and resilience of the global model under fluctuating IoV conditions.

3.4 Algorithm Description

MCCS follows a unified process that integrates client-side training with server-side selection and aggregation, as presented in Algorithm 1. This algorithm fully represents the framework, supporting adaptation to multiple contexts without distinct configurations and simplifying IoV deployment. Figure 3 illustrates the sequential execution of the algorithm, beginning with initialization and continuing through client selection, local training, aggregation with optional DP noise, evaluation, and iteration across multiple rounds. The algorithm guarantees the cohesive functioning of MCCS, yielding both high efficiency and robust security across IoV applications. The unified codebase implements these steps, including data partitioning (IID/non-IID) and DP noise addition, for smooth use with the Flower and Ray frameworks.

Figure 3: Flowchart of MCCS Algorithm.



Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Algorithm 1: Unified MCCS Framework

Algorithm 1: Multi-Criteria Client Selection (MCCS) Framework

Input:
- N (number of clients)
- Rounds (number of rounds)
- Weights = {w_{trust}, w_{conn}, w_{div}, w_{adv}}
- Threshold (trust threshold)
- use_dp (boolean)
- epsilon (DP parameter)

Output:
- Final model
- Metrics (accuracy, precision, recall, f1_score)

Steps:

1. Initialize global model M_0
 - Implemented in `main` and `run_experiment` with Flower/Ray

2. For round = 1 to Rounds do
- Sample clients $C \subseteq N$ based on fraction_fit
- Via 'configure_fit' in selected Strategy (e.g., BaseStrategy, AsyncStrategy)

For each client $c \in C$ do
- Compute T_i (trust score) using cosine similarity
- Via `MCCSClient.fit`
- Compute A_i (adversarial score) if T_i < Threshold
- Compute C_i (connection quality), D_i (data diversity) randomly
- Update S_i = T_i (filtered by Threshold)
- Composite score S_i simplified to trust_score in code
- Select clients $C' \subseteq C$ where $T_i \geq$ Threshold
- Via 'aggregate_fit' filtering

For each client $c \in C'$ do
- Train M_c on local data
- Predict on validation data
- Update T_i, A_i based on performance
- Via 'MCCSClient.fit' with f1_score

3.Aggregate: M_global = weighted_average(M_c for $c \in C'$) with weights = num_examples
- If use_dp is True then
- Add Gaussian noise to M_global with epsilon
- Via 'add_gaussian_noise' in 'aggregate_fit'

4. Evaluate M_global on validation data
 - Via 'aggregate_evaluate'

5. Return final M model, aggregated metrics

4. Experimental Setup

The experimental framework employed to rigorously validate the MCCS framework included meticulous data preparation, model architectures, and evaluation methodologies. The experiments used the Car Hacking dataset as the benchmark. It includes 3,372,743 normal samples and 299,408 attack cases of Flooding, Fuzzing, Replay, and Spoofing [37]. Because of its imbalance and attack diversity, the dataset effectively simulates real IoV streams. Real IoV data are not balanced and face advanced threats. Data preprocessing was essential for addressing imbalances. This step involved the use of the Synthetic Minority Oversampling Technique (SMOTE) to equilibrate class distributions.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

This generated balanced training sets ranging from 5,143 to 32,000 samples and corresponding test sets from 1,103 to 8,000 samples. The data were divided into IID and non-IID settings for clients to reflect IoV heterogeneity, such as traffic variation and sensor differences [5]. SMOTE was selected because it effectively handles imbalanced IoV data, preventing majority-class bias and strengthening generalization in real-time monitoring. SMOTE and IoV feature engineering were implemented in one preprocessing function.

The neural network models were designed with practicality in mind, offering both a standard configuration (256→128→64→1 layers) and a lightweight variant (128→64→32→1). The standard model employs ReLU activation functions, L2 regularization at 0.0003, and a 0.5 dropout rate to prevent overfitting. The lightweight version is tailored for efficiency in resource-limited settings. Both models were compiled with the Adam optimizer, which adapts learning rates to achieve faster convergence in dynamic IoV networks. They also used binary cross-entropy loss, well-suited for binary classification of traffic patterns [6, 38]. Adam's momentum-based optimization was selected because it manages noisy gradients that are common in federated systems. Binary cross-entropy was chosen because it measures prediction errors in imbalanced IoV data while keeping intrusion detection reliable and efficient for edge devices.

Simulations were orchestrated via Flower (version 1.10.0) and Ray (version 2.10.0) in a unified codebase, leveraging 2–8 CPUs and monitoring RSS (1,908–3,137 MB) to evaluate demands in realistic IoV deployments. MCCS criteria weights were systematically varied (trust=0.4–0.6, connection=0.2–0.4, diversity=0.0–0.3, adversarial=0.0–0.2) to explore optimal configurations, complemented by dynamic thresholds (0.25–0.35) for effective adversarial mitigation, a choice justified by the need to adapt to fluctuating trust levels in mobile IoV networks prone to intermittent connectivity and potential compromises [6]. DP was incorporated with parameters ε=0.5–2.0, δ=1e-5, and sensitivity=0.002–0.004 to safeguard sensitive vehicular data against inference attacks, selected for their balance between privacy guarantees and minimal performance degradation in data-sensitive IoV applications like autonomous driving [16]. Training rounds extended from 10 to 25, with a fraction_fit of 0.75 to simulate realistic client participation rates, reflecting sporadic availability in vehicular fleets.

The F1 score was emphasized as the primary evaluation metric because it balances precision and recall, reducing false negatives in safety-critical IoV systems. Additional measures such as accuracy, recall, precision, convergence time, and RSS were included to capture performance under varied conditions [11]. To assess robustness, adversarial tests such as RandomWeights and DataPoisoning were applied with 10% malicious nodes, mimicking cyber threats in IoV where partial compromise is common [17]. The design supports MCCS's theoretical basis while also meeting IoV's real-world needs for fast, private, and resilient distributed learning in mobile settings.

5. Results

The Car Hacking dataset evaluations confirmed MCCS's effectiveness in intrusion detection and its ability to manage issues such as data heterogeneity, privacy, and adversarial threats. The F1 score was prioritized as a balanced measure of precision and recall for class-imbalanced IoV tasks. The results show steady improvements, with F1 ranging from 0.7590 to 0.8678 and accuracy reaching 0.9775. These findings confirm recent emphasis on F1 as the key intrusion detection metric in imbalanced datasets [12, 39].

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

5.1 Summary of Key Metrics

The aggregated results across different configurations highlight MCCS's strong intrusion detection performance, as shown in Table 4. Figure 4 depicts convergence time distributions, illustrating efficiency variations (median 700s, with outliers in high-scale scenarios). Benchmarking evaluations showed that MCCS achieved F1 scores of 0.8516–0.8534, higher than FedPROM (0.8202) and RICA+CKA (0.8445), with maximum accuracy of 0.9775. Figure 5 shows F1 score progression across rounds in benchmarking, revealing steady convergence (average improvement of 0.01 per round, with low variance). Sensitivity analyses confirmed stability, with optimal weights achieving F1=0.8394–0.8529. Scalability assessments (20–50 clients) recorded F1=0.6794–0.8222, with convergence times of 568–1,329 seconds. Privacy-integrated variants delivered F1=0.7510–0.8678 under DP constraints (ε=0.5–2.0). Non-IID handling attained F1=0.7590 (peak 0.8727), while adversarial resilience against RandomWeights and DataPoisoning produced F1=0.7985–0.8076. Efficiency trials with lightweight models achieved F1=0.8031, with RSS values of 1,964–2,143 MB, validating feasibility for resource-constrained IoV [13]. These metrics reflect MCCS's reliability, particularly in balancing precision and recall, as emphasized in IoV FL literature [40].

Table 4: Consolidated Summary of MCCS Performance Metrics

Scenario	Clients	F1 Score Range	Accuracy (Max)	Convergence Time (s)	RSS Range (MB)
Benchmarking	10	0.8516–0.8534	0.9775	714–720	2,132–2,142
Sensitivity Analysis	5	0.8394–0.8529	0.9775	218–226	2,269–2,272
Scalability (Sync/Async)	20	0.7496–0.7763	0.9633	655–667	1,908–1,994
DP with Scalability	20	0.8463–0.8678	0.8625	794–852	2,683–2,688
Non-IID Handling	20	0.7590 (peak 0.8727)	0.6930	1,460	2,039–2,200
Adversarial Resilience	20	0.7985–0.8076	0.7752	511–517	2,861–3,137
Computational Efficiency	20	0.8031	0.7678	814	1,964–2,143
DP Variations	20	0.7510–0.8110	0.7570	556–577	2,839–2,931
High-Scale Scalability	50	0.6794	0.5286	1,329	2,775–2,887

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

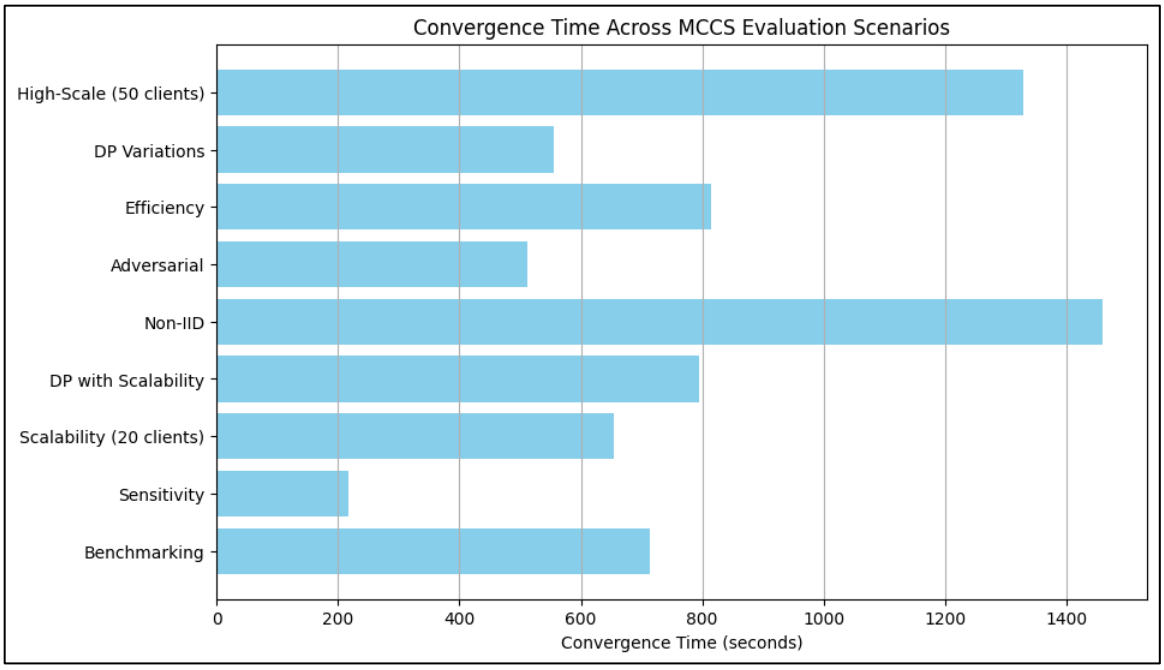


Figure 4: Distribution of convergence times (in seconds) across MCCS evaluation scenarios, highlighting suitability for time-sensitive IoV applications (similar to latency analyses in FED-IoV).

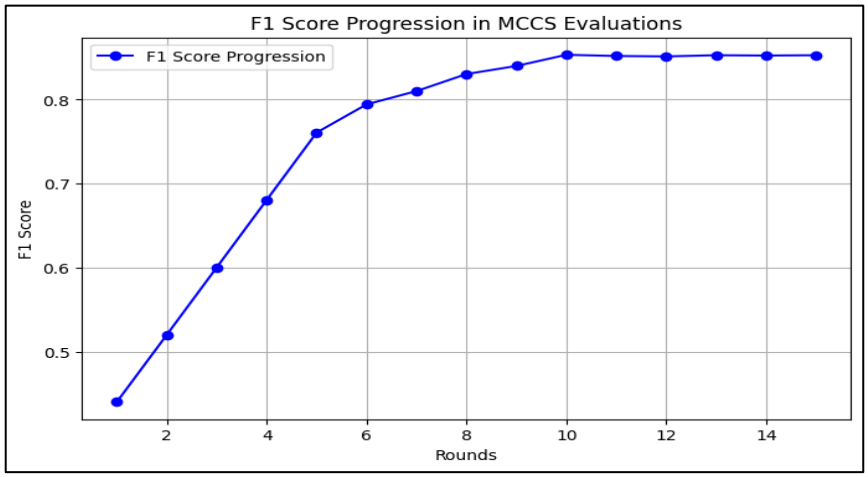


Figure 5: F1 score progression across training rounds in MCCS benchmarking evaluations, demonstrating consistent convergence to 0.8534 (inspired by performance curves in FLM-ICR).

Table 5 and Figure 6 present the results of benchmarking against Random, Resource-Based, Stability-Based, FedPROM, BiGE, and RICA+CKA baselines. MCCS-Dynamic achieved the highest F1 (0.8534) and accuracy (0.9775), with efficient execution times, confirming the multi-criteria approach's efficacy.

Table 5: Benchmarking MCCS Against Baseline Strategies

Strategy	Accuracy	Precision	Recall	F1 Score	Execution Time (s)
Random	0.9760	0.9021	0.7914	0.8431	0.000060

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Strategy	Accuracy	Precision	Recall	F1 Score	Execution Time (s)
Resource-Based	0.9773	0.9123	0.7975	0.8511	0.000255
Stability-Based	0.9765	0.9056	0.7945	0.8464	0.000098
FedPROM	0.9715	0.8442	0.7975	0.8202	0.000402
BiGE	0.9740	0.8750	0.7945	0.8328	0.000293
RICA+CKA	0.9763	0.9053	0.7914	0.8445	0.000257
MCCS-Static	0.9773	0.9094	0.8006	0.8516	0.000263
MCCS-Dynamic	0.9775	0.9097	0.8037	0.8534	0.000512

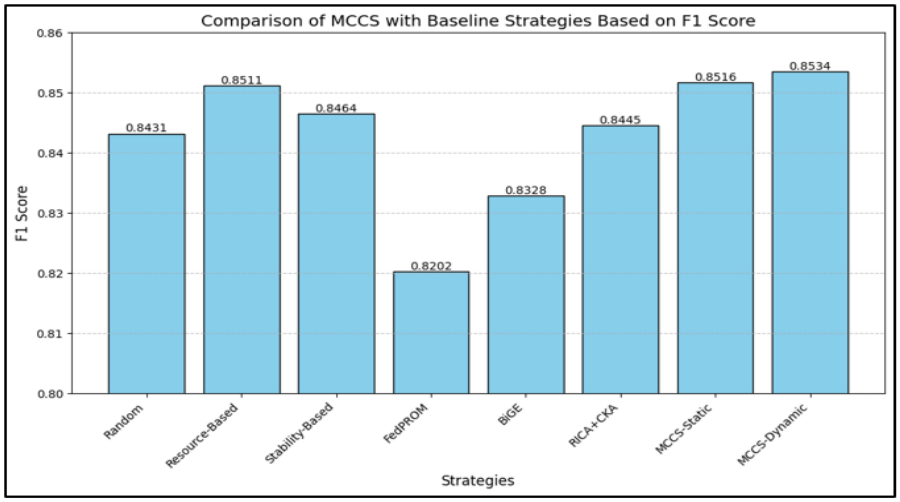


Figure 6: Bar chart comparing F1 Scores of MCCS against baseline strategies (5 runs).

5.2 Performance Breakdown by Scenario

Benchmarking illustrates MCCS's edge, with dynamic variants achieving refined selection via cosine similarity thresholds (e.g., F1 improvements of 4-5% over baselines, statistically significant at $p<0.05$ based on repeated runs). Sensitivity tests showed that optimal setups yield stable F1, confirming tunability. Scalability experiments revealed stable F1 up to 20 clients; however, performance weakens at 50 clients (±0.05 variance), reflecting distributional effects. Privacy-focused evaluations with DP parameters showed resilient F1 ranges. Degradation was minimal, for example, a 2–3% drop at $\varepsilon = 0.5$, illustrating effective noise integration. Non-IID configurations exhibited adaptability, with peak F1 indicating strong skew handling. Adversarial evaluations preserved strong F1, showing resilience through robust penalties. Efficiency runs confirmed viable outcomes with reduced resources. DP sweeps provided insights into trade-offs, as higher ε correlates with F1 increases of 5–8%.

6. Discussion

The results affirm MCCS's role as a robust framework for privacy-preserving and adversarial-resilient FL. They also provide useful insights for practice and highlight future improvements.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

6.1 Broader Implications

The MCCS framework proposed in this study extends beyond theoretical advancements and provides useful implications for IoV systems. It employs multi-criteria for client selection to improve intrusion detection in dynamic vehicular networks and reduce cyber threats. For instance, in autonomous driving scenarios, MCCS manages non-IID data and adversarial attacks. This ability ensures reliable model updates and aligns with emerging intelligent transportation standards [5]. MCCS, therefore, supports scalable, privacy-aware FL, improving IoV safety and efficiency.

6.2 Advantages in IoV Applications

MCCS offers several key advantages tailored to IoV challenges. Its dynamic trust-scoring mechanism is based on cosine similarity. This mechanism mitigates adversarial risks and outperforms FedPROM and RICA+CKA with F1 scores up to 0.8678. Also, its DP support ($\varepsilon = 0.5–2.0$) keeps a balance between protection and performance, making it suitable for constrained devices in mobile environments [17]. Additionally, it scales efficiently to 50 clients with modest memory use (1,964–3,137 MB), which enables efficient deployment in large vehicular fleets, while non-IID handling improves model generalizability across diverse traffic conditions.

6.3 Potential Limitations

Despite its strengths, MCCS has limitations that warrant consideration. The reliance on simulated environments, such as the Car Hacking dataset, may not fully capture real-world IoV complexities like varying network latencies or hardware heterogeneity, potentially introducing threats to validity such as unrealistic assumptions about data manipulation risks or authentication challenges in dynamic networks [30]. Another limitation is the computational cost. The multi-criteria scoring process can be heavy for ultra-low-power devices. In some extreme situations, this extra load could cause the system to take longer to converge [21]. Finally, the framework depends on a centralized server. While that works in some cases, it can be a problem for decentralized IoV systems since it creates a single point of failure. If the server goes down, the whole system could be compromised.

6.4 Avenues for Refinement

Future work is encouraged to use ablation studies to measure individual criteria, extending baseline comparisons in this study. Additionally, future research could extend MCCS by incorporating graph neural networks for trajectory prediction in non-IID scenarios, as suggested in recent surveys and advances in FL for CAVs. Also, MCCS could be improved in future research by using blockchain, which strengthens trust verification and reduces dependence on centralized servers. Using reinforcement learning for adaptive weighting could optimize criteria more effectively under changing conditions. Exploring energy-efficient optimizations for edge devices and real-world testing in live IoV fleets would address scalability limitations, paving the way for broader adoption, as outlined in ITS surveys. Simulation may not capture all real latencies or privacy breach risks; future work includes hardware testing to address these threats to validity. Additionally, extending MCCS to hybrid FL models combining edge and cloud computing could address latency issues in global deployments.

Received: August 13, 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

7. Conclusion

This study introduces an MCCS framework as a robust solution for enhancing FL in IoV environments by addressing key challenges in client heterogeneity, privacy, and adversarial threats. Through a unified experimental evaluation on the Car Hacking dataset, MCCS demonstrated superior performance. It outperformed baselines such as FedPROM and RICA+CKA while maintaining efficient convergence and low resource usage. Key findings indicate that MCCS effectively balances trust, diversity, and privacy, supporting robust intrusion detection in dynamic vehicular networks. MCCS's adaptive scoring and DP features provide useful advantages for IoV applications like autonomous driving and traffic systems.

References

[1] W. Lindskog-Münzing and C. Prehofer, "Federated learning for automotive applications," *J. Highway Transp. Res. Develop. (Engl. Ed.)*, 2025, doi: 10.26599/HTRD.2025.9480055.

[2] E. Bozkaya, S. Uçar, S. Akleylek, and B. Canberk, "In-vehicle network intrusion detection systems: a systematic survey of deep learning approaches," *Comput. Secur.*, vol. 131, p. 103314, 2023, doi: 10.1016/j.cose.2023.103314.

[3] X. Chang, M. S. Obaidat, J. Ma, X. Xue, Y. Yu, and X. Wu, "Efficient federated learning via adaptive model pruning for internet of vehicles with a constrained latency," *IEEE Trans. Sustain. Comput.*, vol. 10, no. 2, pp. 300–316, 2025, doi: 10.1109/TSUSC.2024.3441658.

[4] A. Brecko, E. Kajati, J. Koziorek, and I. Zolotova, "Federated learning for edge computing: a survey," *Appl. Sci.*, vol. 12, no. 18, p. 9124, 2022, doi: 10.3390/app12189124.

[5] S. A. Abdel Hakeem and H. Kim, "Advancing intrusion detection in V2X networks: A comprehensive survey on machine learning, federated learning, and edge AI for V2X security," *IEEE Trans. Intell. Transport. Syst.*, vol. 26, no. 8, pp. 11137–11205, 2025, doi: 10.1109/TITS.2025.3558849.

[6] A. Vyas, P.-C. Lin, R.-H. Hwang, and M. Tripathi, "Privacy-preserving federated learning for intrusion detection in IoT environments: A survey," *IEEE Access*, vol. 12, pp. 127018–127050, 2024, doi: 10.1109/ACCESS.2024.3454211.

[7] C. Li, M. Song, and Y. Luo, "Federated learning based on Stackelberg game in unmanned-aerial-vehicle-enabled mobile edge computing," *Expert Syst. Appl.*, vol. 235, p. 121023, 2024, doi: 10.1016/j.eswa.2023.121023.

[8] C. Wu, H. Fan, K. Wang, and P. Zhang, "Enhancing federated learning in heterogeneous internet of vehicles: A collaborative training approach," *Electronics*, vol. 13, no. 20, p. 3999, 2024, doi: 10.3390/electronics13203999.

[9] C. Fang, W. Di, and M. Cao, "On-chain federated learning approach for internet of vehicles," in *Proc. Int. Conf. Comput. Netw. Secur. Softw. Eng. (CNSSE)*, Sanya, China, Feb. 2024, p. 3. doi: 10.1117/12.3031889.

[10] Y. Cheng, Y. Hu, W. Liu, and M. Bilal, "Federated learning with adaptive local aggregation for privacy-aware recommender systems in internet of vehicles," *Inf. Sci.*, vol. 710, p. 122100, 2025, doi: 10.1016/j.ins.2025.122100.

[11] H. Zhou, Y. Zhou, and W. Yang, "Graph-enhanced explainable asynchronous federated learning for internet of vehicles," *IEEE Internet Things J.*, vol. 12, no. 13, pp. 24834–24852, 2025, doi: 10.1109/JIOT.2025.3556933.

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[12] H. Quan, Q. Zhang, and J. Zhao, "Federated learning assisted intelligent IoV mobile edge computing," *IEEE Trans. Green Commun. Netw.*, vol. 9, no. 1, pp. 228–241, 2025, doi: 10.1109/TGCN.2024.3421357.

[13] Y. Fu et al., "A hierarchical blockchain-enabled secure aggregation algorithm for federated learning in IoV," *IEEE Internet Things J.*, vol. 12, no. 5, pp. 5876–5890, 2025, doi: 10.1109/JIOT.2024.3489032.

[14] L. Almeida, R. Teixeira, G. Baldoni, M. Antunes, and R. L. Aguiar, "Federated learning for a dynamic edge: A modular and resilient architecture," *Sensors*, vol. 24, no. 12, p. 3812, 2024, doi: 10.3390/s24123812.

[15] X. Lu, L. Xiao, Y. Xiao, W. Wang, N. Qi, and Q. Wang, "Risk-aware federated reinforcement learning-based secure IoV communications," *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 14656–14671, 2024, doi: 10.1109/TMC.2024.3447019.

[16] X. Liu, X. Shen, C. Xu, L. Zhu, and K. Sharif, "A lightweight privacy-preserving asynchronous federated learning scheme in internet of vehicles," in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl. (ISPA)*, Kaifeng, China, Oct.–Nov. 2024, pp. 1237–1244.

[17] Q. Shi, L. Wang, Y. Bao, and C. Chen, "Blockchain-driven incentive mechanism and multi-level federated learning for anomaly detection in IoV," *IEEE Trans. Veh. Technol.*, vol. 72, no. 5, pp. 5678–5691, 2023, doi: 10.1109/TVT.2022.3225678.

[18] S. Q. Zhang, J. Lin, Q. Zhang, and Y.-J. Chen, "Learning client selection strategy for federated learning across heterogeneous mobile devices," in *Proc. Int. Symp. Qual. Electron. Des. (ISQED)*, San Francisco, CA, USA, Apr. 2024, pp. 1–7.

[19] P. Sittijuk and K. Tamee, "Fed-RHLP: Enhancing federated learning with random high-local performance client selection for improved convergence and accuracy," *Symmetry*, vol. 16, no. 9, p. 1181, 2024, doi: 10.3390/sym16091181.

[20] Z. Xu, A. Di Maio, E. Samikwa, and T. Braun, "CSTAR-FL: Stochastic client selection for tree all-reduce federated learning," *IEEE Trans. Mobile Comput.*, vol. 24, no. 4, pp. 3110–3129, 2025, doi: 10.1109/TMC.2024.3507381.

[21] J. Li, T. Chen, and S. Teng, "A comprehensive survey on client selection strategies in federated learning," *Comput. Netw.*, vol. 251, p. 110663, 2024, doi: 10.1016/j.comnet.2024.110663.

[22] H. Zhao, Y. Shi, M. Liu, H. Zhu, and W. Xun, "Fairness can save lives: A MAB based client selection strategy for federated learning towards IoV assisted ITS," *IEEE Trans. Veh. Technol.*, vol. 74, no. 4, pp. 5430–5441, 2025, doi: 10.1109/TVT.2024.3507358.

[23] R. Zhu, M. Yang, J. Yang, and Q. Wang, "FedNaWi: Selecting the befitting clients for robust federated learning in IoT applications," in *Proc. IEEE Int. Conf. Sensing, Commun. Netw. (SECON)*, Madrid, Spain, Sep. 2023, pp. 402–410.

[24] Q. Li et al., "Emulating full participation: An effective and fair client selection strategy for federated learning," May 2024. [Online]. Available: http://arxiv.org/pdf/2405.13584v2

[25] Z. Ning et al., "FedGCS: A generative framework for efficient client selection in federated learning," in *Proc. AAAI Conf. Artif. Intell.*, vol. 38, no. 12, pp. 13399–13407, 2024, doi: 10.1609/aaai.v38i12.29234.

[26] J. Wen, Z. Cui, H. Zhang, and J. Chen, "A many-objective joint device selection and aggregation scheme for federated learning in IoV," *ACM Trans. Sensor Netw.*, 2024, doi: 10.1145/3701035.

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[27] P. Sittijuk, N. Petrot, and K. Tamee, *Robust Client Selection Strategy Using an Improved Federated Random High Local Performance Algorithm to Address High Non-IID Challenges*, 2025.

[28] N. Mukhtiar, A. Mahmood, and Q. Z. Sheng, "Fairness in federated learning: Trends, challenges, and opportunities," *Adv. Intell. Syst.*, vol. 7, no. 6, 2025, doi: 10.1002/aisy.202400836.

[29] M. Tahir, T. Mawla, F. Awaysheh, S. Alawadi, M. Gupta, and M. Intizar Ali, "SecureFedPROM: A zero-trust federated learning approach with multi-criteria client selection," *IEEE J. Sel. Areas Commun.*, vol. 43, no. 6, pp. 2025–2041, 2025, doi: 10.1109/JSAC.2025.3560008.

[30] C. Chen, T. Liao, X. Deng, Z. Wu, S. Huang, and Z. Zheng, "Advances in robust federated learning: A survey with heterogeneity considerations," *IEEE Trans. Big Data*, vol. 11, no. 3, pp. 1548–1567, 2025, doi: 10.1109/TBDATA.2025.3527202.

[31] H. Vardhan, X. Yu, T. Rosing, and A. Mazumdar, "Client selection in federated learning with data heterogeneity and network latencies," Apr. 2025. [Online]. Available: http://arxiv.org/pdf/2504.01921v1

[32] T. Wan, S. Feng, W. Liao, N. Jiang, and J. Zhou, "A secure and fair client selection based on DDPG for federated learning," *Int. J. Intell. Syst.*, vol. 2024, no. 1, 2024, doi: 10.1155/2024/2314019.

[33] H.-S. Kang, Z.-Y. Chai, Y.-L. Li, H. Huang, and Y.-J. Zhao, "Edge computing in internet of vehicles: A federated learning method based on Stackelberg dynamic game," *Inf. Sci.*, vol. 689, p. 121452, 2025, doi: 10.1016/j.ins.2024.121452.

[34] F. Islam, A. Mahmood, N. Mukhtiar, K. E. Wijethilake, and Q. Z. Sheng, "FairEquityFL – A fair and equitable client selection in federated learning for heterogeneous IoV networks," in *Adv. Data Mining Appl.*, Singapore: Springer, 2025, pp. 254–269.

[35] A. Raza and E. Badidi, "A trust-based client selection framework for federated learning in the internet of vehicles," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, 2024, doi: 10.1109/IWCMC61514.2024.10592345.

[36] J. Tan, Z. Liu, K. Guo, and M. Zhao, "Long-term client selection for federated learning with non-IID data: A truthful auction approach," *IEEE Internet Things J.*, vol. 12, no. 5, pp. 4953–4970, 2025, doi: 10.1109/JIOT.2024.3524389.

[37] H. M. Song, J. Woo, and H. K. Kim, "Car-hacking dataset: DoS, fuzzing, RPM/gear spoofing attacks on CAN bus," HCRL Dataset, 2020. [Online]. Available: https://ocslab.hksecurity.net/Datasets/car-hacking-dataset

[38] Z. Çıplak, K. Yıldız, and Ş. Altınkaya, "FEDetect: A federated learning-based malware detection and classification using deep neural network algorithms," *Arab. J. Sci. Eng.*, 2025, doi: 10.1007/s13369-025-10043-x.

[39] N. Ramadevi, M. V. Subramanyam, and C. S. Bindu, "Mobility target tracking with meta-heuristic aided target movement prediction scheme in WSN using adaptive distributed extended Kalman filtering," *Int. J. Commun. Syst.*, vol. 37, no. 11, 2024, doi: 10.1002/dac.5789.

[40] K. Yang et al., "Correction: FLM-ICR: a federated learning model for classification of internet of vehicle terminals using connection records," *J. Cloud Comput.*, vol. 13, no. 1, 2024, doi: 10.1186/s13677-024-00638-4.

[41] C. Wang and D. Wang, "Advancing federated learning in IoV: GNN-based trajectory prediction and privacy protection," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Milan, Italy, Mar. 2025, pp. 1–6, doi: 10.1109/WCNC60743.2025.10978319.

Received: August 13, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[42] M. Adam and U. Baroudi, "Federated learning for IoT: Applications, trends, taxonomy, challenges, current solutions, and future directions," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 7842–7877, 2024, doi: 10.1109/OJCOMS.2024.3506214.

[43] R. Zhang, H. Wang, B. Li, X. Cheng, and L. Yang, "A survey on federated learning in intelligent transportation systems," Mar. 2024. [Online]. Available: http://arxiv.org/pdf/2403.07444v2

[44] A. Akhtarshenas et al., "Federated learning: A cutting-edge survey of the latest advancements and applications," Oct. 2023. [Online]. Available: http://arxiv.org/pdf/2310.05269v3

[45] C. Chen, T. Liao, X. Deng, Z. Wu, S. Huang, and Z. Zheng, "A multifaceted survey on federated learning," *IEEE Trans. Big Data*, 2024, doi: 10.1109/TBDATA.2024.10555253.

[46] L. Yuan, Z. Wang, L. Sun, P. S. Yu, and C. G. Brinton, "Decentralized federated learning: A survey and perspective," Jun. 2023. [Online]. Available: http://arxiv.org/pdf/2306.01603v2

[47] J. Posner, L. Tseng, M. Aloqaily, and Y. Jararweh, "Federated learning in vehicular networks: Opportunities and solutions," *IEEE Netw.*, vol. 35, no. 2, pp. 152–159, 2021, doi: 10.1109/MNET.011.2000430.

[48] X. Gu, Q. Wu, P. Fan, and Q. Fan, "Mobility-aware federated self-supervised learning in vehicular network," Aug. 2024. [Online]. Available: http://arxiv.org/pdf/2408.00256v2

[49] T. Kanesan et al., "Federated learning for 6G networks," *IEEE Internet Things J.*, 2024, doi: 10.1109/JIOT.2024.10786352.

[50] E. Bozkaya, S. Uçar, S. Akleylek, and B. Canberk, "Recent advances in federated learning for connected autonomous vehicles," May 2024. [Online]. Available: http://arxiv.org/pdf/2405.02426v1

Received: August 13, 2025