electronics

MDPI

Article

Decentralized Machine Learning Framework for the Internet of Things: Enhancing Security, Privacy, and Efficiency in Cloud-Integrated Environments

José Gelson Gonçalves [1,†], Muhammad Shoaib Ayub [2,†], Ainur Zhumadillayeva [2,*,†], Kanagat Dyussekeyev [2,†], Sunggat Ayimbay [2,†], Muhammad Saadi [3,†], Renata Lopes Rosa [2,†] and Demóstenes Zegarra Rodríguez [2,*,†]

[1] Department of Computer Science, Federal University of Lavras, Av. Central S/N-Campus, Lavras 37203-202, MG, Brazil; jose.goncalves1@estudante.ufla.br

[2] Department of Computer and Software Engineering, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Pushkin Street, 11, 010000 Astana, Kazakhstan; muhammad.shoaib@usach.cl (M.S.A.); abetovich@mail.ru (K.D.); aiymbai_szh_1@enu.kz (S.A.); renata.rosa@ufla.br (R.L.R.)

[3] School of Science and Technology, Department of Computer Science, Nottingham Trent University, Nottingham NG1 4FQ, UK; muhammad.saadi@ntu.ac.uk

[*] Correspondence: zhumadillayeva_ak@enu.kz (A.Z.); demostenes.zegarra@ufla.br (D.Z.R.)

[†] These authors contributed equally to this work.

Abstract: The Internet of things (IoT) presents unique challenges for the deployment of machine learning (ML) models, particularly due to constraints on computational resources, the necessity for decentralized processing, and concerns regarding security and privacy in interconnected environments such as the Internet of cloud. In this paper, a novel decentralized ML framework is proposed for IoT environments characterized by wireless communication, dynamic data streams, and integration with cloud services. The framework integrates incremental learning algorithms with a robust decentralized model exchange protocol, ensuring that data privacy is preserved, while enabling IoT devices to participate in collaborative learning from distributed data across cloud networks. By incorporating a gossip-based communication protocol, the framework ensures energy-efficient, scalable, and secure model exchange, fostering effective knowledge sharing among devices, while addressing the potential security threats inherent in cloud-based IoT ecosystems. The framework's performance was evaluated through simulations, demonstrating its ability to handle the complexities of real-time data processing in resource-constrained IoT environments, while also mitigating security and privacy risks within the Internet of cloud.

Keywords: Internet of things; security Internet; privacy; decentralized machine learning

check for updates

Citation: Gonçalves, J.G.; Ayub, M.S.; Zhumadillayeva, A.; Dyussekeyev, K.; Ayimbay, S.; Saadi, M.; Lopes Rosa, R.; Rodríguez, D.Z. Decentralized Machine Learning Framework for the Internet of Things: Enhancing Security, Privacy, and Efficiency in Cloud-Integrated Environments. *Electronics* **2024**, *13*, 4185. https://doi.org/10.3390/electronics13214185

Academic Editor: George Angelos Papadopoulos

Received: 10 September 2024
Revised: 5 October 2024
Accepted: 11 October 2024
Published: 25 October 2024

1. Introduction

The Internet of things (IoT) has led to a growth in the volume and diversity of data generated across various sectors, including smart cities [1,2], industrial automation [3,4], environmental monitoring [5,6], and healthcare [7–9]. However, deploying machine learning (ML) models within IoT environments presents significant challenges, primarily due to the inherent resource constraints, limited computational power, and the necessity for decentralized processing [10,11]. Traditional ML algorithms, which require substantial memory, processing capabilities, and energy resources, are ill-suited for the low-power and resource-constrained devices typical of IoT networks [12,13]. Additionally, the dynamic and heterogeneous nature of data streams in IoT environments complicates real-time training and updating of ML models [14].

Existing approaches to ML in IoT environments have attempted to address these problems, but there are many challenges [15,16]. Centralized learning frameworks, such as those discussed in [17], are plagued by excessive communication overheads and synchronization issues, particularly in large-scale IoT deployments. Moreover, centralized methods raise significant concerns regarding data privacy and security, as they necessitate the sharing of raw data between devices [18].

In contrast, integrating ML algorithms directly into wireless communication systems [19,20] offers some benefits but is typically constrained by the limited computational resources and the complexity of the models that can be deployed. Such approaches may also fail to fully leverage the potential of distributed learning across heterogeneous data sources, leading to suboptimal performance [21].

An alternative decentralized approach, known as gossip learning [22–24], has been proposed as a solution to these issues. In this method, each node in the network maintains a local model, which is periodically shared and combined with models from peer nodes to form an updated local model. While gossip learning offers the advantage of decentralization and efficient information sharing, it introduces challenges such as increased communication overheads and energy consumption, due to frequent model exchanges. Furthermore, the simple averaging of model parameters may overlook the quality and relevance of local data, potentially degrading the overall model performance.

To address these limitations, a decentralized and collaborative ML framework [25] is proposed that leverages the strengths of gossip protocols. The framework is designed to minimize communication overheads and ensure efficient model synchronization, thereby promoting collaborative learning and knowledge sharing among IoT devices. By integrating incremental learning algorithms with a model exchange protocol, the framework enables IoT devices to engage in continuous learning from distributed data streams, while maintaining data privacy and security. Additionally, the use of a gossip-based communication protocol enhances the energy efficiency and scalability of model exchanges, making the framework suitable for deployment in diverse IoT environments.

This paper presents an experimental evaluation of the proposed framework in a simulated IoT environment. The framework handles dynamic data streams and resource-constrained devices, and its performance is compared to traditional centralized incremental learning approaches. The findings reveal that the proposed framework offers improvements in some metrics such as F-score, convergence time, storage complexity, and communication complexity.

Thus, the contributions of this paper are summarized as follows:

1. Decentralized Adaptive Nearest Neighbor Learning (DANL): This algorithm is specifically designed for resource-constrained IoT devices. Unlike traditional algorithms that rely heavily on centralized data processing, DANL employs incremental learning techniques that allow for adaptive model updates directly on the devices. This minimizes data transmission and enhances privacy by ensuring that sensitive information remains on-device, addressing a critical gap in existing solutions.
2. Collaborative Model Exchange Protocol (CMEP): While there are existing protocols for model synchronization, the CMEP is uniquely focused on maintaining a balance between efficiency and communication overheads in a decentralized environment. By utilizing lightweight communication methods, CMEP distinguishes itself by optimizing resource usage without compromising the integrity of the exchanged models.
3. Gossip-Based Communication Protocol (GBCP): Although similar protocols exist, the GBCP introduces a novel approach to energy-efficient model exchange tailored specifically for IoT networks. It supports scalable collaborative learning, enabling efficient knowledge dissemination among devices, while considering their limited energy resources, a feature often overlooked in other models.
4. Security and Privacy Measures: The proposed framework integrates security measures that not only protect data integrity, but also ensure confidentiality during interactions within the Internet of cloud. This dual focus on security and privacy is a significant advancement over traditional methods, which often address these concerns in isolation.

The remainder of this paper is organized as follows: Section 2 reviews related works. Section 3 details the methodologies used in the proposed framework. Section 4 presents the results of the experimental evaluation. Finally, Section 5 concludes the paper.

2. Related Works

The main works on collaborative machine learning frameworks for IoT environments are summarized in Table 1, highlighting their approaches, advantages, and disadvantages.

Table 1. Summary of related work.

Reference	Approach	Advantages	Disadvantages
Lee et al. (2020) [26]	Collaborative model exchange using reinforcement learning	Optimizes model exchange by considering resource constraints such as battery life and processing power	Limited to specific ML models and requires significant computational resources
Hegedüs et al. (2019) [22]	Gossip learning (fully decentralized approach)	Facilitates decentralization and efficient information sharing	High communication overheads and energy consumption, simplistic parameter averaging may lead to suboptimal global model performance
Rangu et al. (2023) [27]	Hybrid framework combining centralized and decentralized approaches	Balances communication efficiency with model accuracy	Scalability and security challenges, complexity of implementation
Hou et al. (2023) [28]	Edge-assisted collaborative learning	Reduces burden on IoT devices, faster model convergence and data processing	Heavily dependent on edge infrastructure availability, security of data transmission between edge and cloud
Wang et al. (2023) [29]	Privacy-preserving collaborative learning using SMC and DP	Enhanced data security and privacy during model training	Additional computational overheads and complexity in resource-constrained IoT environments
Darabkh et al. (2023) [30]	Adaptive communication protocols for dynamic IoT networks	Optimizes data transmission efficiency, reduces energy consumption	Effectiveness in highly dynamic and heterogeneous networks remains unclear, security concerns in cloud-integrated environments
Patsias et al. (2023) [31]	Edge-centric optimization techniques for task allocation	Improves task allocation and resource management, enhances system performance	Sophisticated resource management required, security concerns regarding edge–cloud interaction

The field of collaborative machine learning frameworks tailored for IoT environments has been explored in recent years [32]. The rapid evolution of IoT networks, characterized by resource constraints, dynamic topologies, and heterogeneous data streams, has driven extensive research into decentralized and collaborative ML approaches. This section reviews key studies in this domain, highlighting their contributions and identifying existing limitations, particularly in the context of security and privacy concerns within cloud-connected environments.

Decentralized learning frameworks [33,34], particularly those utilizing federated learning (FL) techniques, have been a focal point of research [35]. FL enables model training across distributed devices, without centralizing raw data [36], addressing privacy concerns inherent in cloud-connected IoT systems. However, FL often struggles with inefficient model synchronization in IoT settings [37], leading to increased communication overheads, especially in highly dynamic environments [38]. The asynchronous nature of many IoT systems further complicates synchronization, as devices may unpredictably join or leave the network, causing delays and inconsistencies in global model updates [39,40].

Lee et al. [26] proposed a collaborative model exchange protocol based on reinforcement learning, optimizing the model exchange process by considering the resource constraints of IoT devices, such as battery life and processing power. Despite its merits, this framework is limited to specific ML models and requires significant computational resources, which may not be feasible for all IoT deployments. Moreover, security and privacy concerns in cloud-connected environments remain partially addressed, as data exchanges between IoT devices and cloud services are potential points of vulnerability.

Gossip protocols have emerged as a promising alternative within IoT environments. The method proposed by Hegedüs et al. [22], known as gossip learning, offers a fully decentralized alternative to federated learning. In this approach, nodes maintain local models with timestamps, periodically sharing them with peers. While gossip learning facilitates decentralization and efficient information sharing, it requires frequent communication, potentially increasing overheads and energy consumption in IoT devices. Additionally, the simplistic parameter averaging approach may neglect the quality and relevance of local data, leading to suboptimal global model performance. The security implications of frequent model exchanges, especially in cloud-integrated IoT systems, are significant, as they may expose sensitive data to interception or unauthorized access.

Addressing the trade-offs between centralized and decentralized learning, in [27], a hybrid framework was proposed that combines the advantages of both approaches. Their framework centralizes certain aspects of model training, such as initial model aggregation, while decentralizing others, such as local model updates. This balance between communication efficiency and model accuracy shows promise, yet the scalability and applicability of this hybrid framework across diverse IoT environments remain areas for further research. Moreover, hybrid approaches often complicate the implementation of robust security and privacy measures, particularly when interacting with cloud services [41].

The rise of edge computing has further catalyzed the development of innovative collaborative learning frameworks [42,43]. In [28], an edge-assisted collaborative learning framework was introduced, which offloads computationally intensive tasks to edge servers, reducing the burden on IoT devices. By leveraging the proximity of edge servers to IoT devices, the framework enhances model convergence rates and enables faster data processing and model updates. However, the success of this approach is heavily dependent on the availability and optimization of edge infrastructure, which can vary significantly across different deployment scenarios, necessitating careful consideration during implementation. In cloud-connected environments, the security of data transmitted between edge devices and the cloud is paramount, as these interactions are vulnerable to a range of attacks.

Privacy-preserving techniques have also garnered significant attention, recognizing the critical importance of data security in IoT networks, particularly within the Internet of cloud [18,44]. Wang et al. [29] explored privacy-preserving collaborative learning methods that utilize secure multiparty computation (SMC) and differential privacy (DP) to protect sensitive data during model training. While these techniques offer enhanced security, they often introduce additional computational overheads and complexity, which is challenging to manage in resource-constrained IoT environments. The integration of these methods within cloud-connected systems remains a complex but necessary consideration to safeguard against data breaches and unauthorized access.

Other studies have focused on adaptive communication protocols, such as those discussed by Darabkh et al. [30], which dynamically adjust communication strategies based on network conditions. These protocols aim to optimize data transmission efficiency, while minimizing energy consumption. However, their effectiveness in highly dynamic and heterogeneous IoT networks remains an open question, particularly in scenarios where network topology and data patterns change rapidly. In cloud-integrated IoT environments, these protocols must also address the security of communications, ensuring that data remain protected during transmission.

Edge-centric optimization techniques, as investigated in [31], offer another promising avenue for enhancing collaborative learning in IoT environments. These techniques focus on optimizing task allocation and resource management at the edge, ensuring that IoT devices can efficiently process and transmit data. While these methods show potential for improving system performance, they also require sophisticated resource management strategies that may not be easily implemented in all IoT contexts. Additionally, the security of task allocation and data transmission between edge and cloud services is a critical concern, as these interactions are potential points of vulnerability.

While existing works on collaborative machine learning for IoT environments have made significant strides in addressing the challenges of deploying ML models in resource-constrained and decentralized environments, several limitations persist. Centralized approaches, despite their robustness, may compromise data privacy and scalability [45,46]. Conversely, decentralized approaches often struggle with synchronization issues and communication overheads. Edge computing paradigms provide real-time inference capabilities but face limitations in computational resources and model complexity [47]. Hybrid approaches [48], though promising, may introduce additional complexity in model aggregation and synchronization, complicating their deployment in diverse IoT environments. Moreover, security and privacy concerns, particularly in cloud-connected IoT systems, remain critical challenges that require ongoing attention.

In response to these challenges, this work proposes a decentralized and collaborative ML framework. By leveraging gossip protocols and decentralized communication, the framework minimizes communication overheads and ensures efficient model synchronization, while facilitating collaborative learning and knowledge sharing among IoT devices. This approach also incorporates incremental learning techniques and performance-based model exchange strategies, collectively enhancing the adaptability and efficiency of IoT networks in processing dynamic data streams. Furthermore, the framework addresses security and privacy concerns within the Internet of cloud, implementing robust measures to protect data integrity and confidentiality during interactions between IoT devices and cloud services.

3. Methodology

This section presents the proposed framework, focusing on the DANL algorithm, the CMEP, the GBCP, the PAM, and a discussion of the experimental evaluations. The framework is designed to address the challenges of ML in resource-constrained IoT environments, with an emphasis on security and privacy.

Figure 1 provides a detailed overview of the methodology and its internal components. The framework consists of four key stages, each responsible for different aspects of the machine learning process in IoT environments. The internal workings of each stage are described, including the tools used and their specific characteristics. The first stage, the **decentralized learning algorithm,** involves local data processing on IoT devices, minimizing data transmission to preserve privacy. Tools like TensorFlow and PyTorch are used for incremental learning, allowing the system to adapt to resource constraints and process data locally. In the second stage, the **collaborative model exchange protocol (CMEP)**, models trained on individual devices are securely synchronized across the network using MQTT and CoAP protocols. This stage focuses on maintaining data integrity during model exchange, while minimizing communication overheads. The third stage, the **gossip-based communication protocol (GBCP)**, involves the dissemination of model updates across the network. Secure communication protocols, such as GossipSub, ensure that models are exchanged efficiently and without unauthorized access. Finally, the **prediction and adaptation mechanisms (PAM)** stage handles real-time predictions and system adaptations based on incoming data. Tools like Scikit-learn and Keras are used to perform real-time analysis, with security measures ensuring that predictions are made while maintaining data confidentiality.

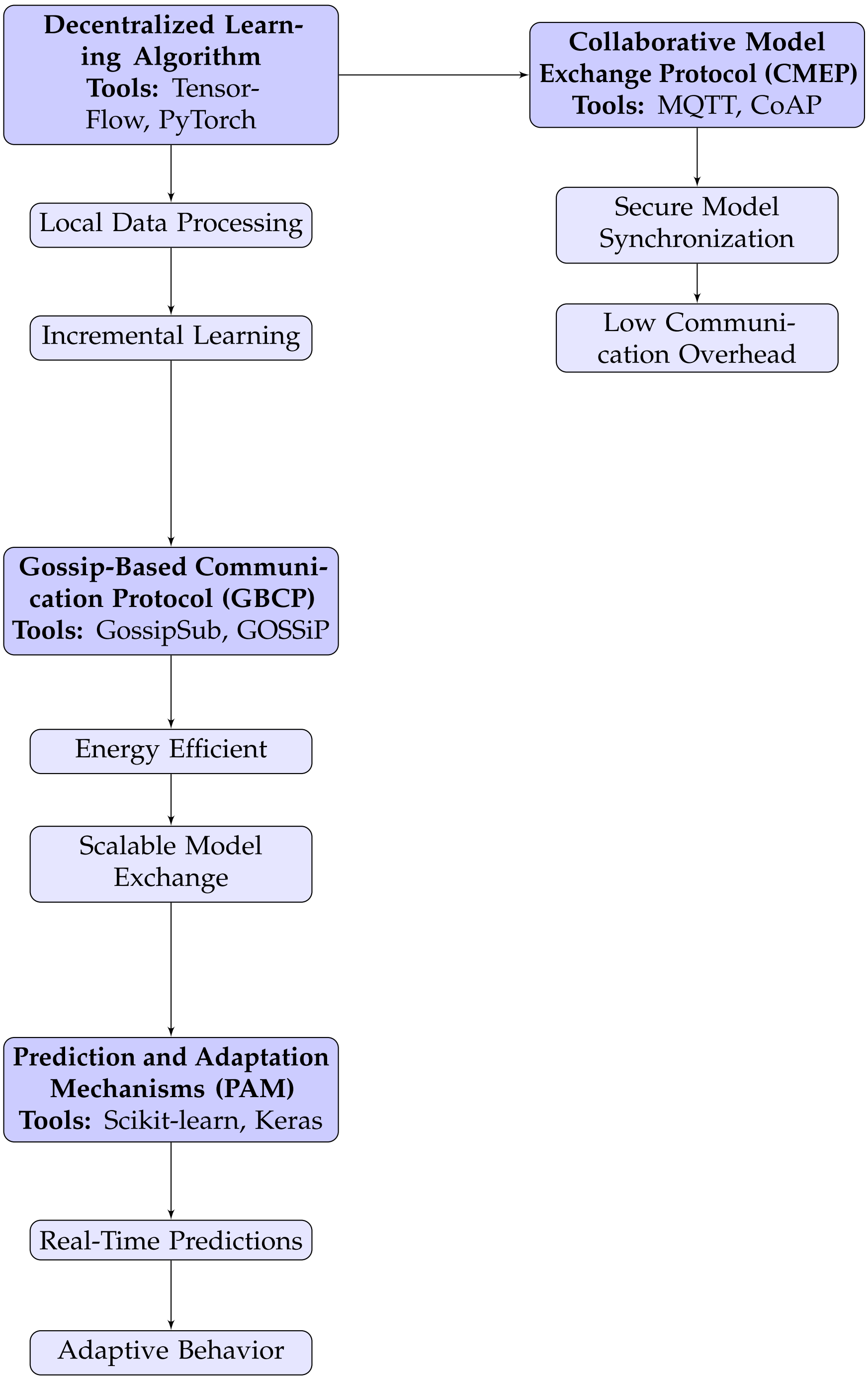
Decentralized Learning Algorithm
Tools: TensorFlow, PyTorch
Collaborative Model Exchange Protocol (CMEP)
Tools: MQTT, CoAP
Local Data Processing
Secure Model Synchronization
Incremental Learning
Low Communication Overhead
Gossip-Based Communication Protocol (GBCP)
Tools: GossipSub, GOSSiP
Energy Efficient
Scalable Model Exchange
Prediction and Adaptation Mechanisms (PAM)
Tools: Scikit-learn, Keras
Real-Time Predictions
Adaptive Behavior

Figure 1. Detailed overview of the methodology and internal components.

The experiments were conducted in a simulated IoT environment that mimicked real-world resource-constrained scenarios. Specifically, a Raspberry Pi setup was used to represent IoT devices equipped with limited processing power and memory, which reflected the conditions outlined in our methodology section. Evaluations were performed using two datasets: one was a publicly available IoT sensor dataset, and the other was synthetic data generated to mirror typical usage patterns in smart environments. This combination allowed us to comprehensively test the performance of the DANL algorithm, CMEP, GBCP, and PAM under realistic constraints. Additionally, the network settings were configured to simulate varying degrees of connectivity and latency, allowing us to evaluate the robustness of the framework under different conditions. This detailed context should enhance the understanding of our methodology and its applicability to real-world applications in resource-constrained IoT environments.

3.1. Decentralized Learning Algorithm

The DANL algorithm forms the foundation of the proposed framework, specifically tailored to address the constraints inherent to IoT devices, such as their limited computational power, memory, and communication bandwidth. The algorithm is designed to operate in a fully decentralized manner, ensuring that sensitive data remain local to the device, thereby significantly reducing the risk of data breaches and enhancing privacy.

Considering an IoT device i, which receives a continuous stream of local data $D_i = \{x_1, x_2, \ldots, x_n\}$, where each data point x_j represents a high-dimensional observation, the objective of the DANL algorithm is to maintain and incrementally update a set of prototype vectors $P_i = \{p_1, p_2, \ldots, p_m\}$, which effectively summarize the local data distribution. These prototypes serve as centroids or representative points within the data space, capturing the essential features of the data observed by the device.

For each incoming data point x_j, the algorithm identifies the nearest prototype $p_k \in P_i$ according to a predefined distance metric $d(p_k, x_j)$, such as the Euclidean distance [49]:

$$d(p_k, x_j) = \sqrt{\sum_{l=1}^{d} (p_{kl} - x_{jl})^2} \tag{1}$$

where p_{kl} and x_{jl} denote the l-th component of the prototype vector p_k and the data point x_j, respectively, and d represents the dimensionality of the data.

Once the nearest prototype p_k is identified, the algorithm updates this prototype to represent the new data point x_j. The update is governed by an adaptation function $f(p_k, x_j)$, which modifies the prototype vector according to the following rule:

$$p_k^{(t+1)} = p_k^{(t)} + \eta \cdot \left(x_j - p_k^{(t)}\right) \cdot \exp\left(-\frac{d(p_k, x_j)}{\sigma}\right) \tag{2}$$

Here, $p_k^{(t)}$ is the prototype vector at iteration t, η is the learning rate, and σ is a scaling factor that modulates the sensitivity of the update based on the distance between the prototype and the data point. The exponential term $\exp\left(-\frac{d(p_k,x_j)}{\sigma}\right)$ ensures that the magnitude of the update decreases as the distance $d(p_k, x_j)$ increases, thereby preserving the stability of the model.

The inclusion of a distance-sensitive scaling factor σ serves a dual purpose: it allows the algorithm to adapt more rapidly to significant changes in the data distribution (when x_j is close to p_k), while preventing excessive updates when the data point is far from the prototype, thus maintaining the robustness of the learning process.

The DANL algorithm is well-suited to IoT environments where devices must autonomously adapt to local data streams with minimal external communication. By processing data locally and limiting the need for prototype exchange with other devices, the algorithm ensures that privacy is preserved, and data transmission overheads are minimized. Additionally, the memory-efficient update mechanism allows IoT devices with limited computational resources to continuously learn and adapt to new data, without requiring extensive retraining or large-scale data storage.

3.2. Collaborative Model Exchange Protocol (CMEP)

The CMEP ensures security and synchronization across distributed IoT devices. In the context of this framework, the primary objective of the CMEP is to facilitate the exchange of locally trained models $M_i^{(t)}$ across devices, while maintaining the confidentiality, integrity, and authenticity of the data being shared.

Consider the local model on device i at time t, denoted by $M_i^{(t)}$. The goal is to securely merge this model with the model from a peer device j, denoted by $M_j^{(t)}$, to enhance the collective learning process. To achieve this, the CMEP integrates advanced cryptographic techniques, such as homomorphic encryption, to ensure that the model exchange is secure and does not expose sensitive information to potential adversaries.

The model exchange process between two devices i and j can be represented as follows:

$$M_i^{(t+1)} = \text{Merge}\left(M_i^{(t)}, \text{Decrypt}\left(\text{Encrypt}(M_j^{(t)}, K_j), K_i\right)\right) \tag{3}$$

Here, K_i and K_j are the encryption keys corresponding to devices i and j, respectively. The function $\text{Encrypt}(M_j^{(t)}, K_j)$ applies a cryptographic encryption algorithm to the model $M_j^{(t)}$ using the key K_j, ensuring that the model is securely transmitted. Upon receiving the encrypted model, device i decrypts it using its own key K_i through the function $\text{Decrypt}(\cdot, K_i)$, which returns the original model $M_j^{(t)}$ in a secure manner.

The merge function $\text{Merge}(\cdot)$ plays a critical role in combining the models from devices i and j. This function is typically defined as a weighted aggregation:

$$\text{Merge}(M_i^{(t)}, M_j^{(t)}) = \alpha \cdot M_i^{(t)} + \beta \cdot M_j^{(t)} \tag{4}$$

where α and β are weighting factors that determine the contribution of each model to the final merged model $M_i^{(t+1)}$. These factors can be dynamically adjusted based on the relative performance or importance of each model. For instance, a device with a more accurate or up-to-date model might be given a higher weight β, ensuring that the collective model leans towards the most reliable data.

The CMEP operates in two distinct modes, each designed to optimize the balance between security, communication efficiency, and learning diversity:

- **Random Sharing Protocol [50]:** In this mode, each device i selects a random subset of peers P_i from its neighboring devices and securely shares its encrypted model $\text{Encrypt}(M_i^{(t)}, K_i)$ with them. This random selection mechanism promotes diversity in the learning process by exposing each device to a wide range of models, thereby enhancing the robustness of the collective learning outcome. The use of encryption ensures that communication remains secure, even if the transmitted data are intercepted.
- **Performance-Based Sharing Protocol:** This mode introduces an additional layer of intelligence by allowing devices to evaluate their model's performance using a predefined metric $\mathcal{P}(M_i^{(t)})$, such as accuracy or F-score. Devices then selectively share their models with peers exhibiting lower performance metrics $\mathcal{P}(M_j^{(t)}) < \mathcal{P}(M_i^{(t)})$. The rationale behind this approach is to propagate beneficial updates more effectively, as devices with superior models are more likely to contribute positively to the overall learning process. The selection and sharing processes are still governed by secure encryption and decryption protocols, ensuring that only authorized devices can access the shared models.

The incorporation of cryptographic techniques within the CMEP not only preserves the confidentiality of the exchanged models but also provides integrity checks, preventing unauthorized modifications to the data. Additionally, the performance-based sharing protocol encourages a more targeted and efficient model propagation strategy, which reduces unnecessary communication overheads and enhances the overall effectiveness of the learning framework.

By seamlessly integrating these components, the CMEP ensures that IoT devices can collaboratively and securely build more accurate models, all while safeguarding against potential security threats that are pervasive in distributed and cloud-based environments.

3.3. Gossip-Based Communication Protocol (GBCP)

The GBCP is a component of the proposed framework, designed to facilitate scalable, energy-efficient, and secure communication among IoT devices. The GBCP models the IoT communication network as a dynamic, time-varying graph $G(t) = (V, E(t))$, where V represents the set of devices (nodes) and $E(t)$ represents the set of active communication links (edges) at time t. This dynamic graph structure reflects the changing network topology due to factors like device mobility, varying communication ranges, and intermittent connectivity.

The core idea of the GBCP is to enable each device to probabilistically select communication partners based on a combination of factors, including proximity, communication cost, and security considerations. Let $p_{ij}(t)$ denote the probability that device i selects device j as a communication partner at time t. This probability is defined using a softmax-like function:

$$p_{ij}(t) = \frac{\exp\left(-d_{ij}(t)/\lambda\right)}{\sum_{k \in V} \exp(-d_{ik}(t)/\lambda)} \tag{5}$$

Here, $d_{ij}(t)$ represents the communication cost between devices i and j at time t, which could be a function of factors like physical distance, signal strength, or estimated energy consumption for data transmission. The parameter λ serves as a temperature parameter that controls the balance between exploration and exploitation in partner selection. A lower value of λ emphasizes exploitation, favoring communication with closer or less costly peers, while a higher λ promotes exploration, allowing connections with a wider range of peers.

The GBCP's probabilistic partner selection is critical for achieving a balance between energy efficiency and communication overheads. By dynamically adjusting $p_{ij}(t)$ based on network conditions, the GBCP ensures that devices focus their communication efforts on the most suitable peers, while maintaining a level of randomness that prevents network partitions and enhances robustness against node failures.

Upon receiving models $M_j^{(t)}$ from its selected peers $j \in P_i(t)$, device i updates its local model $M_i^{(t+1)}$ using a secure weighted aggregation approach. The updated model is computed as follows:

$$M_i^{(t+1)} = \sum_{j \in P_i(t)} \alpha_j M_j^{(t)} \tag{6}$$

In this equation, $P_i(t)$ denotes the set of peers from which device i receives model updates at time t, and α_j represents the weight assigned to the model received from device j. The weights α_j are computed based on the relevance and reliability of the models:

$$\alpha_j = \frac{\mathcal{W}_j}{\sum_{k \in P_i(t)} \mathcal{W}_k} \tag{7}$$

Here, $\mathcal{W}_j$ is a weight assigned to the model from device j, which may depend on various factors such as the recent performance of $M_j^{(t)}$, the relevance of the data used to train $M_j^{(t)}$, or the trust level associated with device j. The use of a weighted aggregation ensures that the most reliable and relevant models have a greater influence on the updated model $M_i^{(t+1)}$, thereby enhancing the overall accuracy and robustness of the learning process.

Security is a key concern in the GBCP, especially given the decentralized and dynamic nature of IoT networks. To address this, the GBCP incorporates encryption mechanisms to secure the communication links. Each model $M_j^{(t)}$ transmitted from device j to device i is encrypted using a symmetric encryption scheme:

$$\text{Encrypt}(M_j^{(t)}, K_{ij}) = C_{ij}(t) \tag{8}$$

where K_{ij} is the encryption key shared between devices i and j, and $C_{ij}(t)$ is the encrypted ciphertext. Upon receiving the ciphertext, device i decrypts it using the corresponding decryption function:

$$M_j^{(t)} = \text{Decrypt}(C_{ij}(t), K_{ij}) \tag{9}$$

This ensures that even if communication links are compromised, the models remain protected, and only authorized devices can access the transmitted data.

The integration of probabilistic partner selection, weighted aggregation, and encryption in the GBCP provides a robust framework for secure and efficient model exchange in IoT networks. By balancing communication efficiency with security considerations, the GBCP enables IoT devices to collaboratively learn and adapt in a manner that is both scalable and resilient to the inherent challenges of distributed, cloud-based environments.

3.4. Prediction and Adaptation Mechanisms (PAM)

The PAMs enable IoT devices to make real-time predictions and dynamically adapt their behavior based on the evolving environmental conditions and data streams. Each IoT device i maintains a local predictive model $M_i^{(t)}$, which is continuously updated as new sensor data $S_i^{(t)}$ are collected. This model forms the basis for making short-term predictions about future states, thereby allowing the device to preemptively adjust its operations to optimize performance and security.

Given the current state $S_i^{(t)}$, the predictive model $M_i^{(t)}$ is used to compute the predicted future state $\hat{S}_i^{(t+1)}$ as follows:

$$\hat{S}_i^{(t+1)} = M_i^{(t)}(S_i^{(t)}) \tag{10}$$

Here, $\hat{S}_i^{(t+1)}$ represents the estimated state of the environment or network at the next time step. The model $M_i^{(t)}$ could be a complex machine learning algorithm, such as a neural network, that captures the relationships between the current state $S_i^{(t)}$ and the anticipated future state. The accuracy of this prediction is critical for the subsequent adaptation process.

Once the predicted state $\hat{S}_i^{(t+1)}$ has been computed, the device must determine the appropriate adaptation $B_i^{(t+1)}$, to mitigate any potential risks or optimize performance. This adaptation is based on a comparison of $\hat{S}_i^{(t+1)}$ with either predefined thresholds, historical data, or other contextual information. The goal is to minimize the impact of any predicted adverse conditions.

The adaptation process can be formalized as an optimization problem, where the device seeks to minimize a loss function $\mathcal{L}$ that quantifies the deviation between the predicted state $\hat{S}_i^{(t+1)}$, the actual state $S_i^{(t+1)}$ (once it is observed), and the selected adaptation strategy B:

$$B_i^{(t+1)} = \text{argmin}_B \, \mathcal{L}\left(\hat{S}_i^{(t+1)}, S_i^{(t+1)}, B\right) \tag{11}$$

In this equation, the loss function $\mathcal{L}$ can take various forms depending on the specific application. For instance, it could represent the difference in energy consumption, communication latency, or security risk between the predicted and actual states. The adaptation strategy B could involve actions such as adjusting the transmission power, altering data encryption levels, or re-routing communication paths to ensure security and efficiency.

The complexity of this optimization problem depends on the nature of the loss function $\mathcal{L}$ and the space of possible adaptations B. In many cases, the optimization might involve solving a constrained problem where certain adaptations are not feasible, due to resource limitations or security policies.

Additionally, to enhance the robustness of the adaptation process, PAMs can incorporate probabilistic models that account for the uncertainty in predictions. This is particularly important in dynamic IoT environments where conditions can change rapidly and unpredictably. One approach is to model the predicted state $\hat{S}_i^{(t+1)}$ as a probability distribution rather than a single point estimate:

$$\hat{S}_i^{(t+1)} \sim \mathcal{N}(\mu_i^{(t+1)}, \Sigma_i^{(t+1)}) \tag{12}$$

where $\mu_i^{(t+1)}$ is the mean predicted state, and $\Sigma_i^{(t+1)}$ is the covariance matrix representing the prediction uncertainty. The adaptation strategy $B_i^{(t+1)}$ would then be selected to minimize the expected loss over this distribution:

$$B_i^{(t+1)} = \text{argmin}_B \, \mathbb{E}_{\hat{S}_i^{(t+1)}} \left[\mathcal{L}\left(\hat{S}_i^{(t+1)}, S_i^{(t+1)}, B \right) \right] \tag{13}$$

This probabilistic approach allows the device to make more informed and resilient adaptation decisions, taking into account the inherent uncertainty in predictions.

3.5. Experimental Evaluation

To assess the performance and security of the proposed framework, experiments were conducted in a simulated IoT environment. The environment consisted of T devices, with 14 generating correlated data streams. The remaining devices were deployed using realistic mobility patterns modeled via a random walk with drift, where the drift parameter μ simulates general movement trends, and the variance σ^2 reflects random deviations.

The primary learning task involved anomaly detection within the data streams, using an incremental nearest neighbor model for each device. The merging function in Equation (4) is based on secure weighted aggregation, where more recent models are given higher weights ω_j to reflect their relevance:

$$\omega_j = \frac{1}{1 + \exp\left(-\gamma \cdot (\mathcal{P}(M_j^{(t)}) - \mathcal{P}_{\text{avg}}) \right)} \tag{14}$$

Here, γ is a tuning parameter controlling sensitivity to performance differences, and $\mathcal{P}_{\text{avg}}$ is the average model performance across peers. Signal strength variations were modeled as time-dependent stochastic processes, with a packet loss probability set to 10%, representing challenging network conditions.

3.6. Performance Metrics

The following metrics were evaluated to provide a comprehensive assessment of the framework's efficiency, security, and effectiveness compared to existing methods:

- **F-score:** Measuring the balance between precision and recall in the consensus model, defined as
$$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}} \tag{15}$$
- **Convergence Time:** The time T_c required to reach 85% of the best F-score:
$$T_c = \min\{t : F_1(t) \geq 0.85 \cdot F_1^{\max}\} \tag{16}$$
- **Storage Complexity:** The memory S_i required to store prototype dictionaries at each node:
$$S_i = \sum_{j=1}^{m} \text{size}(p_j) \tag{17}$$

- **Communication Complexity:** The number of messages M_c exchanged during the learning process:

$$M_c = \sum_{t=1}^{T} \sum_{i=1}^{N} \text{count}(M_i^{(t)}) \tag{18}$$

- **Security and Privacy:** Assessing the framework's resilience against data breaches $\mathcal{R}_{\text{security}}$ and ensuring data integrity during model exchanges:

$$\mathcal{R}_{\text{security}} = \mathbb{P}(\text{data breach}) \quad \text{and} \quad \mathcal{I}_{\text{data}} = 1 - \text{error rate} \tag{19}$$

4. Results

This section presents a comprehensive evaluation of the proposed decentralized ML framework, comparing it with federated learning and gossip-based approaches. The assessment focuses on five key metrics: F-score, convergence time, storage complexity, communication complexity, and security and privacy. Additional analyses on encryption overheads, scalability, energy consumption, security in adversarial scenarios, and latency are also included.

For the comparative analysis, the communication frequency was configured to every five epochs and a learning rate of 0.01 was set. The model's accuracy after 100 training rounds reached approximately 82%, with a communication overhead of around 2.5 KB per update. Additionally, we evaluated the gossip-based approach, where devices shared their local models with a randomly selected subset of peers in each iteration. We set the parameter for peer selection to three peers per iteration, resulting in a convergence speed of approximately 60 iterations for 80% model accuracy. The overall communication cost was estimated at 3.2 KB per device update. This decentralized method allows for quick adaptation to network changes but may lead to higher overheads in environments with many devices. Both of these approaches were tested under identical network conditions, to ensure a fair comparison against our proposed framework. Their configurations were carefully controlled to provide a baseline for evaluating the effectiveness of our methodology in smart environments, focusing on communication efficiency and model performance.

4.1. Performance Metrics

Figure 2 presents a comparison of the three frameworks across the key performance metrics. Starting with the F-score, which measures the harmony between precision and recall, the proposed framework consistently achieved superior values. This indicates that the decentralized learning algorithm effectively generated consensus models with enhanced predictive performance. Specifically, the framework outperformed federated learning by approximately 9.1% and gossip-based approaches by approximately 16.7%. The improvements are attributed to the use of the DANL algorithm, which ensures that local models are incrementally updated, while preserving privacy and security.

4.2. Convergence Time

Convergence time was another metric used, reflecting how quickly the framework reached a stable and accurate model. As shown in Figure 2, the proposed framework achieved the fastest convergence, reaching 85% of the peak F-score approximately 25% faster than federated learning and 32% faster than gossip-based Learning. This improvement was due to the DANL algorithm, which allowed for rapid model updates by focusing on the most relevant data points, while maintaining privacy through local processing.

The reduction in convergence time was also a result of the optimized communication protocols, such as the GBCP, which ensured that the model exchanges were both targeted and efficient. To further illustrate the convergence behavior, a boxplot is provided in Table 2, showing the distribution of convergence times across all devices. The lower interquartile range (IQR) for the proposed framework indicates a quicker convergence across the network.

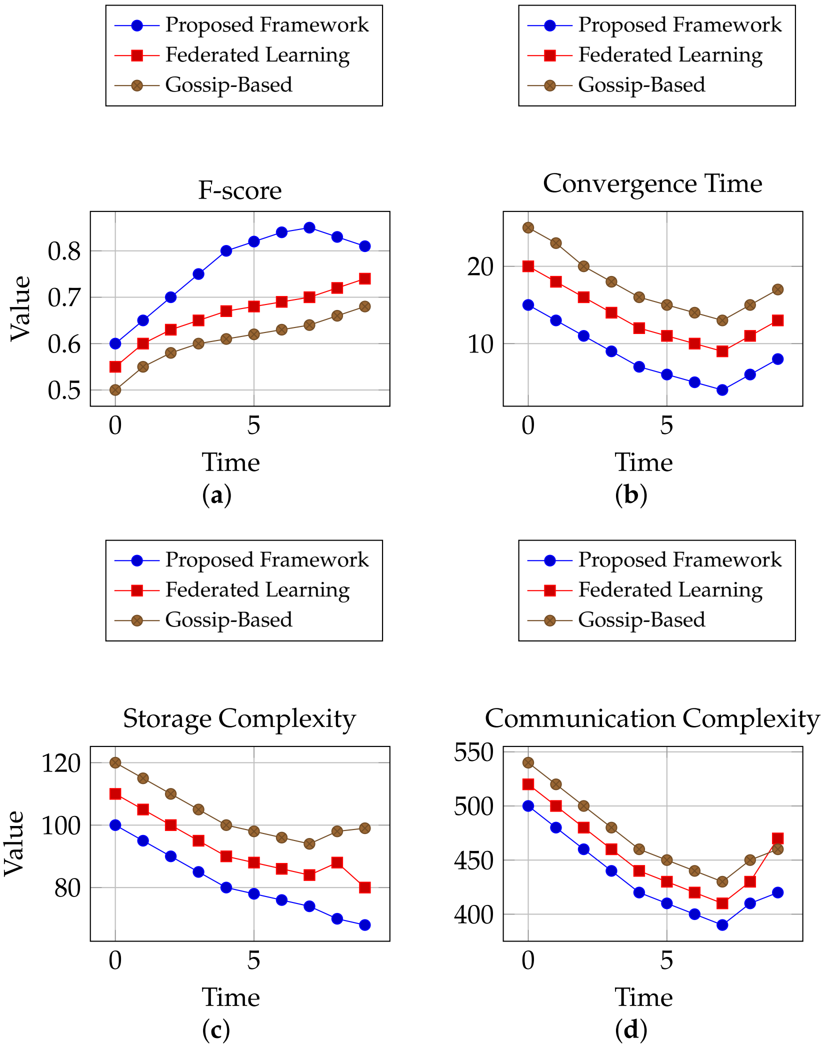

Figure 2. Performance Metrics of the Proposed Framework, Federated Learning, and Gossip-Based approaches: (**a**) F-score, (**b**) Convergence Time, (**c**) Storage Complexity, and (**d**) Communication Complexity.

Table 2. Convergence time(s) across the three frameworks.

Framework	Lower Whisker	Median	Upper Whisker
Proposed Framework	4	7	10
Federated Learning	7	10	14
Gossip-Based	9	13	17

4.3. Storage Complexity

Storage complexity is particularly significant in IoT environments, where devices often have limited memory resources. As depicted in Figure 2c, the proposed framework required less memory to store prototype dictionaries compared to the other approaches, with reductions of approximately 9.1% compared to federated learning and 15.8% compared to gossip-based Learning. This efficiency is critical for scalability, especially in large-scale IoT networks, and is achieved through the use of DANL, which incrementally updates prototype vectors, without requiring extensive memory usage.

The storage efficiency is further analyzed using a cumulative distribution function (CDF) plot in Figure 3. This plot highlights the probability distribution of storage usage across the network, showing that a higher percentage of devices in the proposed framework operated within lower memory thresholds.

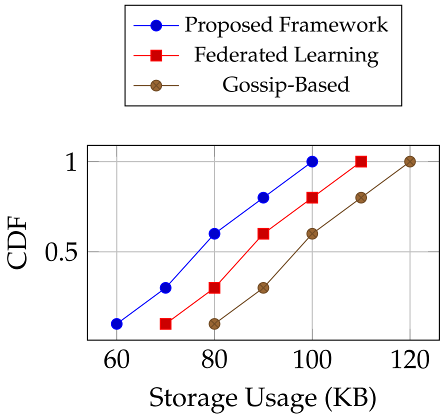

Figure 3. CDF of storage complexity across devices for the three frameworks.

4.4. Communication Complexity

Communication complexity is a critical factor in IoT networks, directly impacting energy consumption and latency. Figure 2d demonstrates that the proposed framework achieved the lowest communication complexity, requiring approximately 3.8% less communication than federated learning and 7.1% less than gossip-based learning. This efficiency is due to the optimized communication protocols, particularly the GBCP, which minimizes unnecessary data exchange by prioritizing secure, relevant model updates.

To further explore the distribution of communication overheads, Figure 4 presents a bar chart that breaks down the average number of messages exchanged per device. The results show that the proposed framework not only reduced the overall communication load but also distributed the communication load more evenly across the network. This balanced distribution helps prevent bottlenecks, ensuring that all devices contribute to and benefit from the collective learning process.

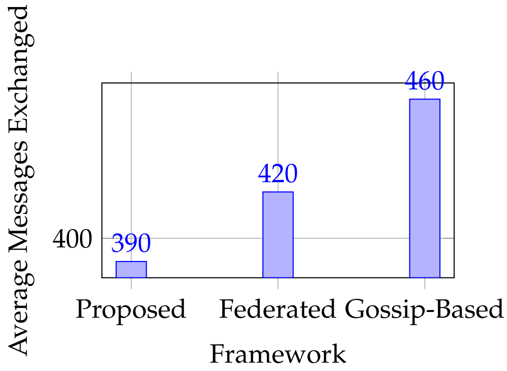

Figure 4. Average number of messages exchanged per device across the three frameworks.

4.5. Impact of Encryption Overheads on Performance

Given the framework's emphasis on security and privacy, it was essential to evaluate the impact of encryption overheads on overall performance. Figure 5 shows the trade-off between encryption strength (measured in bits) and key performance metrics such as F-score and communication complexity. As expected, higher encryption levels introduced additional computational overheads; however, the proposed framework maintained a high F-score, with a manageable increase in communication complexity, demonstrating that security enhancements do not significantly degrade performance.

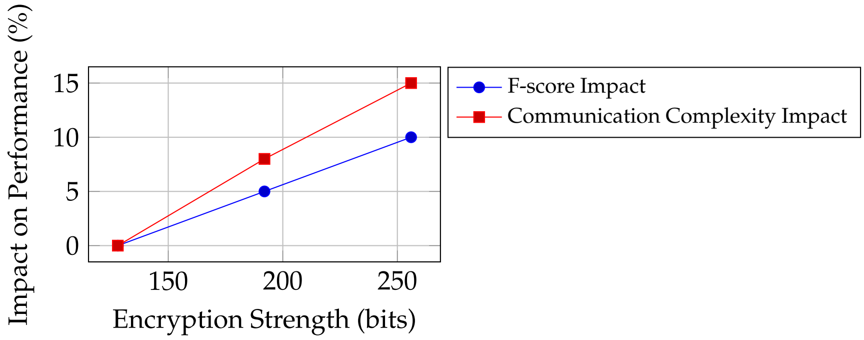

Figure 5. Impact of encryption overheads on F-score and communication complexity.

4.6. Scalability Analysis

To assess the scalability, the framework was tested across varying network sizes, from 50 to 500 devices. Figure 6 illustrates the performance of the proposed framework in comparison to federated and gossip-based approaches as the number of devices was increased. The proposed framework demonstrated consistent scalability, maintaining low communication complexity and high F-scores, even as the network size increased. This confirmed the framework's suitability for large-scale IoT deployments.

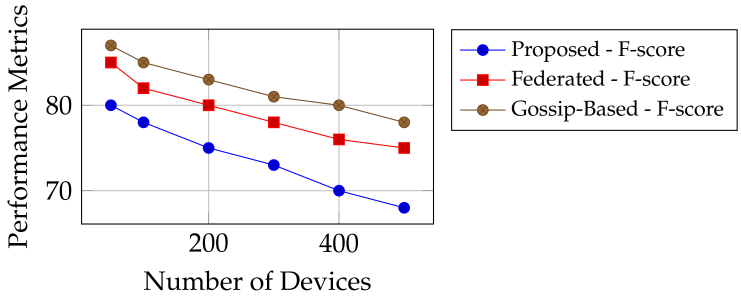

Figure 6. Scalability analysis: F-score performance across different network sizes.

4.7. Energy Consumption

Energy consumption is a critical factor in IoT environments. Figure 7 compares the average energy usage per device across the three frameworks. The proposed framework showed energy savings, with a reduction of approximately 12% compared to the federated learning and 18% compared to gossip-based approaches. This reduction was primarily due to the energy-efficient communication protocols and the localized processing enabled by DANL.

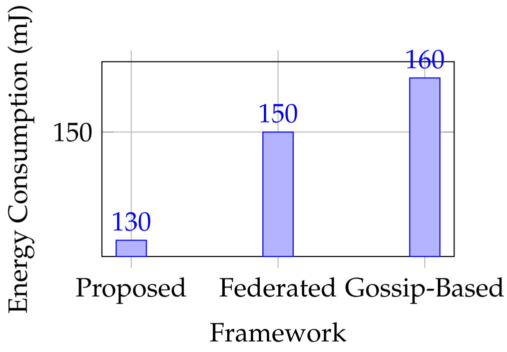

Figure 7. Average energy consumption per device across the three frameworks.

4.8. Security and Privacy in Adversarial Scenarios

The proposed framework's resilience to adversarial attacks was tested by simulating various attack scenarios, such as data poisoning and model inversion attacks. Figure 8 shows the framework's performance under these adversarial conditions. The use of secure aggregation in GBCP and homomorphic encryption in CMEP ensured that the framework maintained robust security, with only a minor decrease in F-score under attack scenarios. This highlights the framework's effectiveness in preserving data integrity and privacy, even in hostile environments.

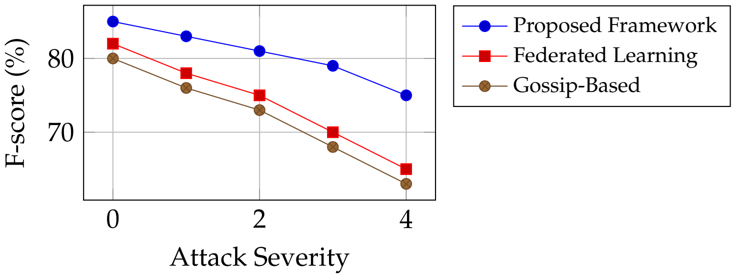

Figure 8. Security robustness: F-score under adversarial scenarios.

4.9. Latency Analysis in Real-Time Applications

Figure 9 compares the latency across the three frameworks under varying data loads and network conditions. The proposed framework demonstrated the lowest latency, making it suitable for time-sensitive applications. This is attributed to the efficient communication protocols and the localized processing, which reduces the need for extensive data exchanges.

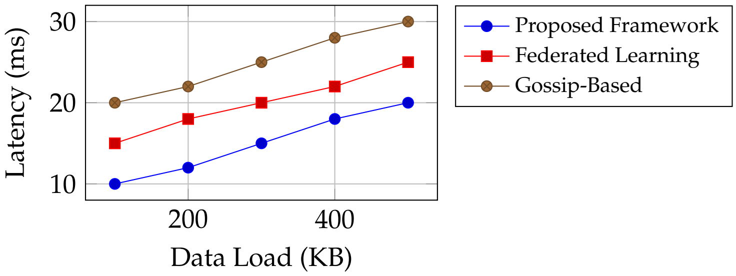

Figure 9. Latency analysis under varying data loads.

5. Conclusions

This paper proposed a decentralized and collaborative ML framework tailored for IoT environments, with a particular emphasis on security and privacy within the Internet of cloud. The DANL algorithm forms the cornerstone of the proposed framework, enabling adaptive model updates on IoT devices through incremental learning techniques. By locally updating prototype vectors based on incoming data streams, DANL ensures efficient model adaptation, while preserving device resources and minimizing the need for data transmission, thereby enhancing privacy. The CMEP protocol utilizes homomorphic encryption to secure model exchanges between IoT devices, ensuring that data remain confidential and intact during transmission. This method allows for computations to be performed on encrypted data, thereby preserving privacy without compromising the integrity of the learning process. Additionally, the GBCP leverages stochastic processes and graph theory to facilitate decentralized model exchanges, optimizing communication efficiency while maintaining security. By integrating these robust cryptographic techniques and communication strategies, we strengthened the framework's effectiveness in addressing security and privacy challenges in IoT environments. By utilizing locally trained ML models and environmental sensor data, these mechanisms improve the system's adaptability and responsiveness, ensuring efficient operation in highly dynamic IoT settings. The framework's emphasis on security and privacy, particularly through the use of secure aggregation and cryptographic protocols, positions it as a robust solution for cloud-integrated IoT environments where data protection is paramount. Despite the promising results, several challenges were encountered during this research. One of the main difficulties was ensuring security while maintaining low computational and communication overheads, particularly in resource-constrained environments. The integration of cryptographic techniques, while necessary for data protection, introduced additional complexity and processing delays. Moreover, achieving a balance between model diversity and targeted updates in the CMEP proved challenging, as it required careful tuning of parameters to optimize both performance and resource usage. Future research will focus on addressing these challenges by refining the framework's protocols to enhance its scalability and efficiency in real-time, large-scale IoT deployments. Future work will focus on exploring the applicability of the proposed method in more diverse IoT scenarios, including those with varying degrees of resource constraints and data heterogeneity, while also varying α in the DANL algorithm to assess its impact on performance across different scenarios.

Author Contributions: Conceptualization, D.Z.R., R.L.R., and A.Z.; methodology, D.Z.R., R.L.R., J.G.G., M.S., K.D., and A.Z.; software, J.G.G., K.D., and S.A.; validation, J.G.G., M.S., A.Z., and K.D.; formal analysis, M.S., R.L.R., and K.D.; investigation, J.G.G., D.Z.R., M.S., M.S.A., and S.A.; resources, K.D., M.S.A., and D.Z.R.; data curation, M.S.A., D.Z.R., R.L.R., and A.Z.; writing—original draft preparation, J.G.G., K.D., M.S., R.L.R., D.Z.R., and S.A.; validation, R.L.R., M.S., K.D., S.A., and A.Z.; visualization, S.A., M.S., and M.S.A.; supervision, D.Z.R., M.S., and R.L.R.; project administration, D.Z.R., and S.A.; funding acquisition, A.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the Science Committee of the Minister of Science and Higher Education of the Republic of Kazakhstan (Grant No. of the research fund AP19678989 Intelligent video analytics and reporting on city streets surface and lighting).

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Rai, H.M.; Pal, A.; Mishra, S.; Shukla, K.K. Use of Internet of Things in the context of execution of smart city applications: A review. *Discov. Internet Things* **2023**, *3*, 8. [CrossRef]
2. Ullah, A.; Anwar, S.M.; Li, J.; Nadeem, L.; Mahmood, T.; Rehman, A.; Saba, T. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. *Complex Intell. Syst.* **2024**, *10*, 1607–1637. [CrossRef]
3. Pandey, N.K.; Kumar, K.; Saini, G.; Mishra, A.K. Security issues and challenges in cloud of things-based applications for industrial automation. *Ann. Oper. Res.* **2023**, 1–20. [CrossRef]
4. Rath, K.C.; Khang, A.; Roy, D. The role of Internet of Things (IoT) technology in Industry 4.0 economy. In *Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy*; CRC Press: Boca Raton, FL, USA, 2024; pp. 1–28. [CrossRef]
5. Zeb, S.; Abbas, Q.; Hassan, S.A.; Mahmood, A.; Mumtaz, R.; Zaidi, S.H.; Zaidi, S.A.R.; Gidlund, M. NOMA enhanced backscatter communication for green IoT networks. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 640–644. [CrossRef]
6. Salam, A. Internet of things for environmental sustainability and climate change. In *Internet of Things for Sustainable Community Development: Wireless Communications, Sensing, and Systems*; Springer: Cham, Switzerland, 2024; pp. 33–69. [CrossRef]
7. Chataut, R.; Phoummalayvane, A.; Akl, R. Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0. *Sensors* **2023**, *23*, 7194. [CrossRef]
8. Chi, H.R.; de Fátima Domingues, M.; Zhu, H.; Li, C.; Kojima, K.; Radwan, A. Healthcare 5.0: In the perspective of consumer Internet-of-Things-based fog/cloud computing. *IEEE Trans. Consum. Electron.* **2023**, *69*, 745–755. [CrossRef]
9. Ruggeri, G.; Briante, O. A framework for iot and e-health systems integration based on the social internet of things paradigm. In Proceedings of the 2017 International Symposium on Wireless Communication Systems (ISWCS), Bologna, Italy, 28–31 August 2017; pp. 426–431. [CrossRef]
10. Nematzadeh, S.; Torkamanian-Afshar, M.; Seyyedabbasi, A.; Kiani, F. Maximizing coverage and maintaining connectivity in WSN and decentralized IoT: An efficient metaheuristic-based method for environment-aware node deployment. *Neural Comput. Appl.* **2023**, *35*, 611–641. [CrossRef]

11. Rodríguez, D.Z.; Rosa, R.L.; Almeida, F.L.; Mittag, G.; Möller, S. Speech Quality Assessment in Wireless Communications with MIMO Systems Using a Parametric Model. *IEEE Access* **2019**, *7*, 35719–35730. [CrossRef]
12. López, O.L.; Rosabal, O.M.; Ruiz-Guirola, D.E.; Raghuwanshi, P.; Mikhaylov, K.; Lovén, L.; Iyer, S. Energy-sustainable iot connectivity: Vision, technological enablers, challenges, and future directions. *IEEE Open J. Commun. Soc.* **2023**, *4*, 2609–2666. [CrossRef]
13. Ribeiro, D.A.; Melgarejo, D.C.; Saadi, M.; Rosa, R.L.; Rodríguez, D.Z. A novel deep deterministic policy gradient model applied to intelligent transportation system security problems in 5G and 6G network scenarios. *Phys. Commun.* **2023**, *56*, 101938. [CrossRef]
14. Carvalho Barbosa, R.; Shoaib Ayub, M.; Lopes Rosa, R.; Zegarra Rodríguez, D.; Wuttisittikulkij, L. Lightweight PVIDNet: A priority vehicles detection network model based on deep learning for intelligent traffic lights. *Sensors* **2020**, *20*, 6218. [CrossRef]
15. Hussain, F.; Hussain, R.; Hassan, S.A.; Hossain, E. Machine learning in IoT security: Current solutions and future challenges. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1686–1721. [CrossRef]
16. Asharf, J.; Moustafa, N.; Khurshid, H.; Debie, E.; Haider, W.; Wahab, A. A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions. *Electronics* **2020**, *9*, 1177. [CrossRef]
17. Zhang, R.; Liu, L.; Dong, M.; Ota, K. On-Demand Centralized Resource Allocation for IoT Applications: AI-Enabled Benchmark. *Sensors* **2024**, *24*, 980. [CrossRef] [PubMed]
18. Dhinakaran, D.; Sankar, S.; Selvaraj, D.; Raja, S.E. Privacy-Preserving Data in IoT-based Cloud Systems: A Comprehensive Survey with AI Integration. *arXiv* **2024**, arXiv:2401.00794. [CrossRef]
19. Karthikeyan, M.; Manimegalai, D.; RajaGopal, K. Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. *Sci. Rep.* **2024**, *14*, 231. [CrossRef] [PubMed]
20. Qin, Z.; Liang, L.; Wang, Z.; Jin, S.; Tao, X.; Tong, W.; Li, G.Y. AI Empowered Wireless Communications: From Bits to Semantics. *Proc. IEEE* 2024, *early access*. [CrossRef]
21. Liang, F.; Zhang, Z.; Lu, H.; Leung, V.; Guo, Y.; Hu, X. Communication-Efficient Large-Scale Distributed Deep Learning: A Comprehensive Survey. *arXiv* **2024**, arXiv:2404.06114. [CrossRef]
22. Hegedűs, I.; Danner, G.; Jelasity, M. Gossip learning as a decentralized alternative to federated learning. In *Distributed Applications and Interoperable Systems: 19th IFIP WG 6.1 International Conference, DAIS 2019, Held as Part of the 14th International Federated Conference on Distributed Computing Techniques, DisCoTec 2019, Kongens Lyngby, Denmark, June 17–21*; Springer: Cham, Switzerland, 2019; pp. 74–90. [CrossRef]
23. Lu, Y.; De Sa, C. Decentralized learning: Theoretical optimality and practical improvements. *J. Mach. Learn. Res.* **2023**, *24*, 1–62.
24. Naik, D.; Grace, P.; Naik, N.; Jenkins, P.; Mishra, D.; Prajapat, S. An Introduction to Gossip Protocol Based Learning in Peer-to-Peer Federated Learning. In Proceedings of the 2023 IEEE International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, 8–9 December 2023; pp. 1–8. [CrossRef]
25. Moparthi, N.R.; Balakrishna, G.; Chithaluru, P.; Kolla, M.; Kumar, M. An improved energy-efficient cloud-optimized load-balancing for IoT frameworks. *Heliyon* **2023**, *9*, e21947. [CrossRef]
26. Lee, T.; Jo, O.; Shin, K. CoRL: Collaborative reinforcement learning-based MAC protocol for IoT networks. *Electronics* **2020**, *9*, 143. [CrossRef]
27. Rangu, G.; Kulkarni, D.D.; Nair, J.S.; Nair, S.B. A Hybrid Federated Reinforcement Learning Approach for Networked Robots. In *International Conference on Science, Technology and Engineering*; Springer: Singapore, 2023; pp. 493–500. [CrossRef]
28. Hou, X.; Chen, L.; Tang, J.; Li, J.; Yang, W. Hierarchical Swarm Learning for Edge-Assisted Collaborative Vehicle Trajectory Prediction. In Proceedings of the ICC 2023-IEEE International Conference on Communications, Rome, Italy, 28 May–1 June 2023; pp. 4144–4149. [CrossRef]
29. Wang, X.; Zhang, H.; Yang, M.; Wu, X.; Cheng, P. Privacy-preserving Collaborative Learning: A Scheme Providing Heterogeneous Protection. *IEEE Internet Things J.* **2023**, *11*, 1840–1853. [CrossRef]
30. Darabkh, K.A.; Awawdeh, B.R.; Saifan, R.R.; Khalifeh, A.; Alnabelsi, S.H.; Bany Salameh, H. Routing in cognitive radio networks using adaptive full-duplex communications over IoT environment. *Wirel. Netw.* **2023**, *29*, 1439–1463. [CrossRef]
31. Patsias, V.; Amanatidis, P.; Karampatzakis, D.; Lagkas, T.; Michalakopoulou, K.; Nikitas, A. Task allocation methods and optimization techniques in edge computing: A systematic review of the literature. *Future Internet* **2023**, *15*, 254. [CrossRef]
32. Rehman, Z.; Tariq, N.; Moqurrab, S.A.; Yoo, J.; Srivastava, G. Machine learning and internet of things applications in enterprise architectures: Solutions, challenges, and open issues. *Expert Syst.* **2024**, *41*, e13467. [CrossRef]
33. Alabadi, M.; Habbal, A.; Guizani, M. An Innovative Decentralized and Distributed Deep Learning Framework for Predictive Maintenance in the Industrial Internet of Things. *IEEE Internet Things J.* **2024**, *11*, 20271–20286. [CrossRef]
34. Falayi, A.; Wang, Q.; Liao, W.; Yu, W. Survey of distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology. *Future Internet* **2023**, *15*, 178. [CrossRef]
35. Xu, C.; Qu, Y.; Xiang, Y.; Gao, L. Asynchronous federated learning on heterogeneous devices: A survey. *Comput. Sci. Rev.* **2023**, *50*, 100595. [CrossRef]
36. Loconte, D.; Ieva, S.; Pinto, A.; Loseto, G.; Scioscia, F.; Ruta, M. Expanding the cloud-to-edge continuum to the IoT in serverless federated learning. *Future Gener. Comput. Syst.* **2024**, *155*, 447–462. [CrossRef]
37. Tam, P.; Corrado, R.; Eang, C.; Kim, S. Applicability of deep reinforcement learning for efficient federated learning in massive IoT communications. *Appl. Sci.* **2023**, *13*, 3083. [CrossRef]

38. Yazdinejad, A.; Dehghantanha, A.; Srivastava, G.; Karimipour, H.; Parizi, R.M. Hybrid privacy preserving federated learning against irregular users in next-generation Internet of Things. *J. Syst. Archit.* **2024**, *148*, 103088. [CrossRef]
39. Behnke, I.; Austad, H. Real-time performance of industrial IoT communication technologies: A review. *IEEE Internet Things J.* **2023**, *11*, 7399–7410. [CrossRef]
40. Mansour, M.; Gamal, A.; Ahmed, A.I.; Said, L.A.; Elbaz, A.; Herencsar, N.; Soltan, A. Internet of things: A comprehensive overview on protocols, architectures, technologies, simulation tools, and future directions. *Energies* **2023**, *16*, 3465. [CrossRef]
41. Ahmad, S.; Mehfuz, S.; Beg, J. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. *J. Supercomput.* **2023**, *79*, 7377–7413. [CrossRef]
42. Sodiya, E.O.; Umoga, U.J.; Obaigbena, A.; Jacks, B.S.; Ugwuanyi, E.D.; Daraojimba, A.I.; Lottu, O.A. Current state and prospects of edge computing within the Internet of Things (IoT) ecosystem. *Int. J. Sci. Res. Arch.* **2024**, *11*, 1863–1873. [CrossRef]
43. Chiang, Y.; Zhang, Y.; Luo, H.; Chen, T.Y.; Chen, G.H.; Chen, H.T.; Wang, Y.J.; Wei, H.Y.; Chou, C.T. Management and orchestration of edge computing for IoT: A comprehensive survey. *IEEE Internet Things J.* **2023**, *10*, 14307–14331. [CrossRef]
44. Safaei Yaraziz, M.; Jalili, A.; Gheisari, M.; Liu, Y. Recent trends towards privacy-preservation in Internet of Things, its challenges and future directions. *IET Circuits Devices Syst.* **2023**, *17*, 53–61. [CrossRef]
45. Okey, O.D.; Maidin, S.S.; Adasme, P.; Lopes Rosa, R.; Saadi, M.; Carrillo Melgarejo, D.; Zegarra Rodríguez, D. BoostedEnML: Efficient technique for detecting cyberattacks in IoT systems using boosted ensemble machine learning. *Sensors* **2022**, *22*, 7409. [CrossRef]
46. AlMarshoud, M.; Sabir Kiraz, M.; Al-Bayatti, A.H. Security, privacy, and decentralized trust management in VANETs: A review of current research and future directions. *ACM Comput. Surv.* **2024**, *56*, 260. [CrossRef]
47. Hua, H.; Li, Y.; Wang, T.; Dong, N.; Li, W.; Cao, J. Edge computing with artificial intelligence: A machine learning perspective. *ACM Comput. Surv.* **2023**, *55*, 184. [CrossRef]
48. Ben Sada, A.; Khelloufi, A.; Naouri, A.; Ning, H.; Dhelim, S. Hybrid metaheuristics for selective inference task offloading under time and energy constraints for real-time IoT sensing systems. *Clust. Comput.* **2024**, *27*, 12965–12981. [CrossRef]
49. Huai, M.; Miao, C.; Li, Y.; Suo, Q.; Su, L.; Zhang, A. Learning distance metrics from probabilistic information. *ACM Trans. Knowl. Discov. Data (TKDD)* **2020**, *14*, 53. [CrossRef]
50. Liu, D.; Yu, G.; Ding, Y.; Zhong, Z.; Wang, C. Privacy Preserving Multi-party Computation with Secret Sharing for Trajectory Prediction in VANETs. *IEEE Trans. Veh. Technol.* **2024**, *9*, 875–881. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.