

Article

Location Privacy Protection in Edge Computing: Co-Design of Differential Privacy and Offloading Mode

Guowei Zhang , Shengjian Zhang, Zhiyi Man, Chenlin Cui and Wenli Hu

School of Cyber Science and Engineering, Qufu Normal University, Qufu 273165, China;
15563118018@qfnu.edu.cn (S.Z.); mzy18661429940@qfnu.edu.cn (Z.M.); cuichenlin@qfnu.edu.cn (C.C.);
hwl-11@qfnu.edu.cn (W.H.)

* Correspondence: zhanggw@qfnu.edu.cn

Abstract: Edge computing has emerged as an innovative paradigm that decentralizes computation to the network's periphery, empowering edge servers to manage user-initiated complex tasks. This strategy alleviates the computational load on end-user devices and increases task processing efficiency. Nonetheless, the task offloading process can introduce a critical vulnerability, as adversaries may infer a user's location through an analysis of their offloading mode, thereby threatening the user's location privacy. To counteract this vulnerability, this study introduces differential privacy as a protective mechanism to obscure the user's offloading mode, thereby safeguarding their location information. This research specifically addresses the issue of location privacy leakage stemming from the correlation between a user's location and their task offloading ratio. The proposed strategy is based on differential privacy. It aims to increase the efficiency of offloading services and the benefits of task offloading. At the same time, it ensures privacy protection. An innovative optimization technique for task offloading that maintains location privacy is presented. Utilizing this technique, users can make informed offloading decisions, dynamically adjusting the level of obfuscation in response to the state of the wireless channel and their privacy requirements. This study substantiates the feasibility and effectiveness of the proposed mechanism through rigorous theoretical analysis and extensive empirical testing. The numerical results demonstrate that the proposed strategy can achieve a balance between offloading privacy and processing overhead.

Keywords: edge computing; differential privacy; task offloading; privacy preserving



Citation: Zhang, G.; Zhang, S.; Man, Z.; Cui, C.; Hu, W. Location Privacy Protection in Edge Computing: Co-Design of Differential Privacy and Offloading Mode. *Electronics* **2024**, *13*, 2668. <https://doi.org/10.3390/electronics13132668>

Academic Editor: Simeone Marino

Received: 26 May 2024

Revised: 2 July 2024

Accepted: 3 July 2024

Published: 7 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The proliferation of intelligent terminals [1] and the Internet of Things (IoT) [2] has catalyzed a significant increase in the variety of terminal applications. This not only enhances users' entertainment experiences but also escalates their demand for robust computing resources and energy on mobile devices. However, the compact design of mobile terminals inherently limits their processing power, storage capabilities, network connectivity, and battery life, often failing to meet the computational needs of users. Despite these limitations, task offloading offers a promising solution, as discussed in the next paragraph. It allows users to transfer computationally intensive tasks from their mobile devices to other systems for processing, thereby reducing the computational load on the devices themselves [3]. Initially, cloud servers were deemed ideal candidates for computational offloading. Over the past decade, the rapid expansion and advancement of cloud computing have equipped these servers with substantial storage and processing capabilities. As a result, they provide an extensive array of resources and services to users of the Internet of Things (IoT). Nonetheless, as the proliferation of resource-constrained mobile devices continues to grow, the limitations of mobile cloud computing [4,5] have become increasingly evident. One of the most pressing challenges faced by mobile users is the latency encountered when exchanging data with cloud servers via wide area networks (WANs). The intrinsic latency

associated with WANs is particularly problematic, as it can lead to significant delays in service provision and negatively impact the user experience. Moreover, mobile cloud computing faces further challenges, such as the potential for privacy breaches and restrictions imposed by the limited bandwidth [6]. As users interact with cloud services, sensitive data may be exposed to unauthorized parties, raising significant concerns regarding data security and user privacy [7]. In addition, the bandwidth limitations of mobile networks can hinder the efficient transmission of data, particularly for applications that require high-speed connectivity. In light of these challenges, the research community and industry stakeholders are exploring alternative solutions that can offer the benefits of cloud computing, while minimizing latency and enhancing data privacy. Edge computing, which brings computation closer to the source of data generation, is emerging as a promising approach for addressing these concerns. By processing data at the network's edge, edge computing can reduce latency, decrease bandwidth usage, and provide a more secure environment for data processing, thus offering a more robust and efficient computing ecosystem for mobile and IoT users.

To protect the location privacy of mobile users, this study proposes a task offloading strategy based on differential privacy [8,9], according to the relationship between the offloading ratio and the user's location. Before the task is offloaded to the edge server, the user makes the task offloading decision according to the real distance to obtain the real offloading ratio, and then uses differential privacy to confuse the user's real offloading ratio. Offloading is performed using the proportion of offloading after the obfuscation.

In order to solve the above problems, relevant scholars have proposed mobile edge computing (MEC) technology [10]. MEC technology migrates computing storage capabilities and business service capabilities to the edge of the network, so that applications, services, and content can be deployed as localized, close, and distributed. Compared with the cloud computing model, users can provide their low latency and low energy consumption computing experience with stronger privacy and security by offloading computing tasks to MEC servers that are physically close to each other [11]. However, the low latency and high efficiency of MEC also put forward new requirements for privacy protection, and the emergence of malicious edge servers also provides more ways for privacy leakage. Therefore, protecting the privacy of mobile users while maintaining low latency and energy consumption is a key issue in MEC task offloading. The main contributions of this paper are summarized as follows.

1. This paper introduces an innovative framework for the offloading of edge computing tasks that ensures robust privacy protection for users, while reducing the energy and latency costs associated with task offloading. The core principle of the framework is to address the issue of protecting the location information of users.

2. By employing differential privacy to obscure offloading ratios to edge servers across various privacy contexts, the framework enables informed offloading decisions. This approach makes it challenging for the edge server to deduce the user's actual location upon receiving anonymized offloading data. The level of obfuscation is dynamically adjusted to reflect current wireless channel conditions and privacy requirements, thereby striking a balance between privacy and computational efficiency.

3. The validity of our method is confirmed by its compliance with the ϵ -differential privacy standard, offering a rigorous theoretical foundation for safeguarding users' location privacy. Moreover, a multitude of comparative experiments utilizing real datasets validate the efficacy of our proposed framework.

The remainder of this paper is organized as follows. Section 2 presents an analysis of the current state of MEC research. Section 3 introduces the system model and background knowledge of this study. Section 4 introduces the DP-based location privacy protection strategy for edge computing. Section 5 presents an analysis of the performance of the proposed strategy. Finally, Section 6 concludes the study and introduces future work.

2. Related Work

Edge computing task offloading has emerged as a focal point of research within the networking domain in recent years. The literature [12] assesses the shift from cloud to edge, especially in mobile contexts, to determine the most effective technology. It synthesizes insights from various studies on cloud and mobile edge computing, and the role of mobility in tech advancement. Existing strategies for task offloading are predominantly concerned with two primary goals: optimizing resource utilization and enhancing privacy safeguards. This manuscript delves into pertinent research and advancements in task offloading from the perspectives of resource efficiency and privacy preservation.

2.1. Resource Optimization

We first present research work on task offloading with the goal of reducing computational latency. The literature [13] proposed a multi-resource collaborative management framework based on asynchronous deep reinforcement learning (A3C algorithm) to solve the problem of task offloading and resource allocation in the vehicle edge computing environment to maximize system utility. Through simulation experiments, it was verified that the proposed method has significant advantages over other schemes in terms of the response delay and system performance. The literature [14] considered the heterogeneous delay constraints and resource competition comprehensively. We aim at minimizing the energy consumption of MDs subject to the individual delay constraints of tasks by jointly optimizing the task offloading and resource allocation in terms of wireless channel and remote computation capacity in a multi-MD MEC system in this paper. Due to the complexity of the primal optimization problem, a heuristic algorithm is devised. In the algorithm, a subset of tasks to be offloaded is incrementally constructed, and the corresponding offloading sub-problem is then repeatedly solved for this task subset using a two-stage algorithm until the total energy consumption can no longer be further reduced. The proposed heuristic algorithm is evaluated against three reference schemes, and the results show that it can save up to 14.20% of energy consumption while guaranteeing the delay requirements of all tasks. Also using heuristics are EAA [15], JODTS [16], and ISSA [17]. The literature [18] proposed a hybrid mobile edge computing (MEC)-enabled computation placement coordinator to solve the problem of high-reliability delivery (HRT) and computation delay minimization (CDM) in heterogeneous vehicle networks (HetVNETs).

Research work on task offloading with the goal of minimizing energy expenditure within a considerable computation delay is described next. Reference [19] introduced a UAV edge computing system aided by RIS, which aims to minimize energy consumption by considering various factors such as the user transmission power, intelligent reflector phase shift matrix, UAV trajectory, computational resource allocation, and the stability of task queues. The paper concludes that the proposed algorithm effectively reduces the system energy consumption while ensuring the stability of the system task queue, offering new insights into minimizing energy consumption in RIS-assisted UAV-MEC systems. The literature [20] proposed a game-theoretic resource management technique, considering the interests of all parties involved, aiming to minimize infrastructure energy consumption, and costs, while ensuring application performance. The resource allocation problem is modeled as a non-cooperative game where customers (SaaS), resource providers (IaaS), and access networks (NaaS) act selfishly according to their own objectives. The literature [21] formulated an optimization problem named STRONG, which aims to minimize the energy consumption of devices (user and helper devices) under various constraints, including the sum of offloading task ratios, offloading times, completion delays, and total energy consumption for offloading and local computing tasks. A two-step solution is presented to address the STRONG problem. First, a low-complexity search-based algorithm is used for selecting the helpers and MEC server. Second, algorithms are developed to provide suboptimal solutions for power allocation to the helper and MEC servers, as well as the offloading task ratios, considering the non-convex nature of the energy minimization problem. Numerical results are provided to validate the effectiveness of the proposed

algorithm. The results demonstrate the efficiency of the approach and the superiority of the cooperative NOMA-based MEC scenario compared with methods without cooperation and other cooperation-based scenarios.

Finally, we introduce the research work that aims to balance the relationship between computation latency and energy cost. The literature [22] proposed an FL-inspired distributed learning framework for computation offloading in VNs. A constrained optimization problem is developed to jointly minimize overall latency and energy consumption. An evolutionary genetic algorithm (GA) is proposed to solve the problem and is compared with benchmarks. The simulation results demonstrate the effectiveness of the proposed approach in terms of the latency and energy consumption. Reference [23] presented a cooperative computation offloading framework in a three-tier multi-server MEC system, considering both competition among multiple MDs and unknown service demand. The proposed SCRACO scheme outperformed the other methods in reducing the average total cost of the system. The literature [24] proposed an MEC cluster-based energy-aware offloading framework that provides efficient 5G-MEC workload orchestration, energy consumption, and cost management. The framework is designed to operate efficiently in a highly scalable domain of computation resources and large workloads.

2.2. Privacy Protection

In recent years, some privacy protection mechanisms for task offloading have been proposed, which are mainly divided into two aspects: privacy problems caused by data interaction and those caused by task offloading characteristics. To address privacy issues caused by traditional data interaction, literature [25] proposed a secure data sharing method under an edge computing framework that combines federated learning and blockchain technology for MIIoT. Federated learning ensures the privacy of nodes, whereas blockchain serves as a decentralized means of storing information about federated learning workers, achieving non-tampering and security. An ocean environment model is constructed in this study, and the analysis based on this model makes the proposed method more applicable to the marine environment. The numerical results from the simulation experiments demonstrate that the proposed scheme can significantly improve learning accuracy while ensuring the safety and reliability of the marine environment. Similarly, LCC [26], PFCEL [27], and NESPS [28] have addressed privacy protection issues in data interaction scenarios. However, the privacy issue in the data exchange scenario is beyond the scope of this paper, which focuses on the privacy leakage problem caused by the task offloading feature.

In [29], an improved CMA-ES algorithm (TADG-CMA-ES) was proposed to address task offloading in vehicle edge computing, considering multiple objectives such as latency, energy consumption, load balancing, and privacy protection. By employing a triple analysis decision variable grouping strategy, the algorithm effectively tackles multi-objective optimization and provides low-latency services while safeguarding user privacy. The experimental results demonstrate that TADG-CMA-ES outperforms existing algorithms across various performance metrics. The literature [30] proposes a novel location privacy-aware task offloading framework (LPA-Offload) designed to protect users' location privacy in mobile edge computing environments, while achieving efficient task offloading. The framework incorporates a location perturbation mechanism, a perturbation region determination mechanism, and an offloading strategy generation mechanism to provide strict privacy protection and adaptively generate offloading strategies based on individual privacy requirements. LPA-Offload has been proven to satisfy (ϵ, δ) -differential privacy and has demonstrated effectiveness in experimental results. The literature [31] presents a caching-based dual K-anonymous (CDKA) location privacy-preserving scheme for edge computing environments. This scheme utilizes edge servers as intermediaries between users and location-based services (LBSs) servers, employing multilevel caching to reduce the load on user devices and dual anonymity to protect location privacy. The study demonstrates that the proposed scheme outperforms existing works in terms of response rate, communication cost, and cache hit ratio, and is robust against privacy offenses from both the edge server

and the LBS server. The literature [32] introduces a strategy known as P2SPA. This strategy is designed to enhance privacy protection for edge nodes (ENs) within edge computing networks. It operates under resource constraints and aims to maximize cost-effectiveness by employing a collaborative ‘end–edge–cloud’ service model. The P2SPA strategy utilizes the analytic hierarchy process (AHP) to quantify privacy protection preferences for user information and selects the optimal EN. It also constructs a pseudo-address selection and updating strategy based on Stackelberg game theory to achieve an optimal pseudo-address update frequency. The effectiveness of the P2SPA strategy is verified through numerical estimations, demonstrating its satisfactory performance in term of both defense effectiveness and cost when compared with existing methods. The literature [33] discusses the development of intelligent logistics, especially the application of unmanned aerial vehicles (UAVs) in the field of logistics, providing efficient, fast, and flexible transportation and distribution solutions. In this paper, the authors use differential privacy and diffusion models to implement secure facial recognition and identity authentication in an edge computing environment to address privacy issues in drone distribution. The literature [34] propose a new federated edge learning framework based on hybrid differential privacy and adaptive compression for industrial data processing. It first completes the adaptive gradient compression preparation, then constructs the industrial federated learning model, and finally makes use of the adaptive differential privacy model to optimize, so as to complete the privacy protection towards the transmission of gradient parameters in industrial environments.

However, the prevailing methods for task offloading in privacy protection merely establish a predefined level of privacy for users and incorporate it as a metric within the overarching optimization objective. These methods fall short of offering a distinct approach for safeguarding user privacy. The results indicate that current methodologies are susceptible to inference attacks and lack rigorous theoretical substantiation to ensure the efficacy of privacy preservation. Furthermore, existing strategies primarily address the leakage of location information for users who are distant from the edge server and subject to suboptimal wireless connectivity. They often overlook the correlation between user location data and the proportion of user task offloading, thereby providing no safeguards for user location information.

Consequently, there is an imperative need to develop novel mechanisms that preserve privacy in task offloading within the realm of edge computing. These mechanisms should not only provide stringent theoretical proof for privacy protection to secure user confidentiality but also optimize task offloading decisions. The quest is for an approach that is robust against potential privacy breaches and adept at making informed task offloading choices, thereby fortifying the privacy and integrity of user data in edge computing environments.

3. System Model and Background Knowledge

In this chapter, we present a structured exposition of the task offloading system model within the edge-computing paradigm. Initially, we delineated the model framework. Subsequently, we address pivotal privacy concerns, namely location privacy, and articulate their respective threat models in the context of task offloading. In this section, we provide a comprehensive overview of the task offloading system model in the context of edge computing. Firstly, we outline the framework of the model. We then discuss critical privacy concerns, focusing on location privacy, and detail the corresponding threat models associated with task offloading. The chapter concludes with an examination of the differential privacy techniques embedded within the proposed privacy protection mechanism. This chapter culminates in an exploration of the differential privacy techniques integrated into our proposed privacy protection mechanism.

3.1. System Model

In this study, we focus on the interaction between edge servers and mobile users in an edge computing framework. The service range of edge servers covers a large number of mobile device users. Users can transfer computational tasks for complex applications

to nearby edge servers to reduce energy consumption and response latency, as shown in Figure 1. This article concentrates on the interplay between edge servers and mobile users within the framework of edge computing. The service scope of edge servers extends to a substantial user base that is equipped with mobile devices. By offloading computationally intensive tasks to proximal edge servers, users can significantly reduce their energy expenditure and response latency, as depicted in Figure 1.

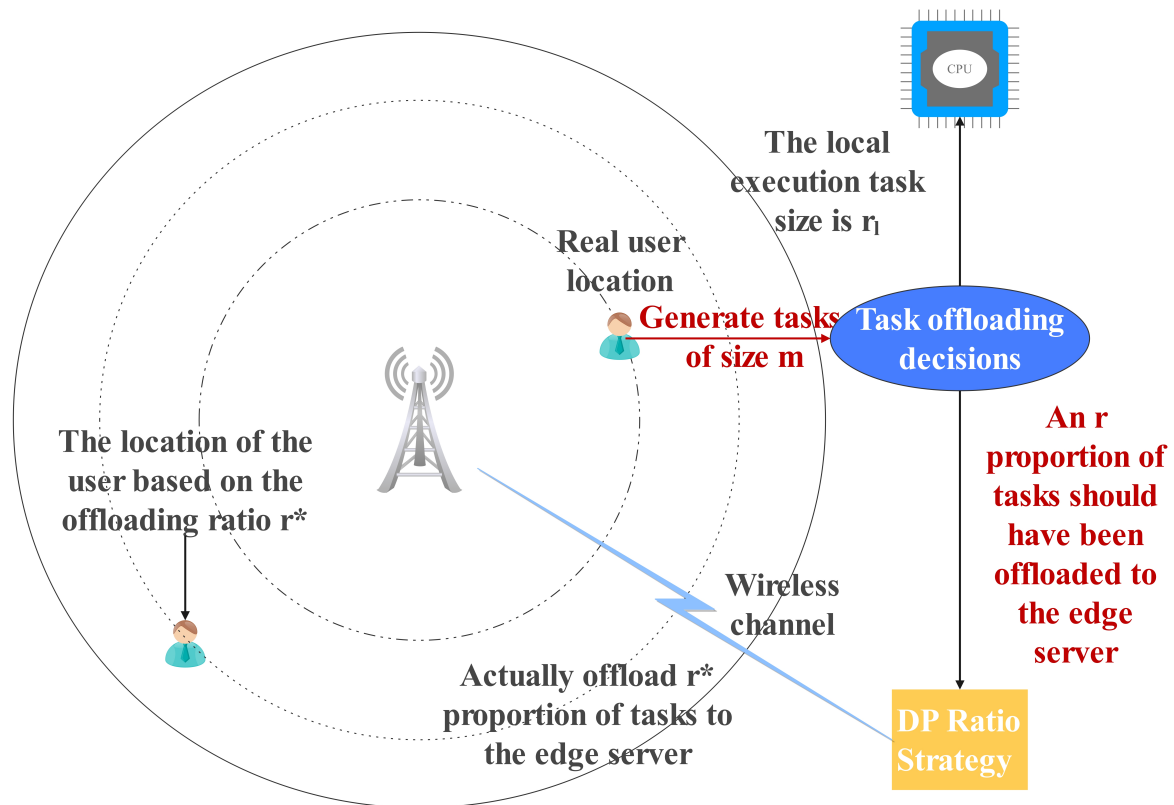


Figure 1. Task offloading framework with location protection in edge computing.

Given the constraints of limited computational resources and battery life on the user's device, the user often opts to upload a portion of their computationally intensive tasks to an edge server for remote processing via a wireless channel, thereby conserving local resources. However, the edge server, while operating with integrity within the edge computing framework, exhibits benign curiosity regarding the mobile user's private information, such as location data. If the volume of tasks generated by the user's device does not correlate with device usage, the edge server can potentially deduce the user's location upon actual task offloading, contingent upon real-time wireless channel conditions.

Assume that the user side generates m bits of computation tasks. The mobile user processes v_l bits of tasks locally and uploads the remaining $v_s = m - v_l$ of the tasks to the edge server for computation. We also define $r_l = v_l/m$ as the proportion of users performing local task processing at moment t , and $r_s = 1 - r_l$ as the proportion of users performing task offloading. Subsequently, this paper presents the local computation model, edge server computation model, and overall computation model in the context of edge computing task offloading.

3.2. Local Computational Models

It is assumed that there are v_l tasks that perform computation locally. Let f_l denote the computational power of the user's mobile device in terms of the number of CPU cycles running per second; the local computational latency is as follows:

$$D_l = \frac{v_l \gamma}{f_l}, \quad (1)$$

where γ represents the number of CPU cycles consumed by the mobile device to complete the task per bit, and $v_l \gamma$ denotes the total number of cycles to complete the task locally. Meanwhile, the energy consumption required to complete v_l tasks on the mobile device is

$$E_l = k f_l v_l \gamma, \quad (2)$$

where k is an intrinsic parameter of the user's mobile device, k is a fixed value, and the value of k differs for different devices.

3.3. Edge Server Computing Models

At timestamp t , it is assumed that the mobile device uploads a portion of the generated task amount v_s bits to the edge server for calculation over a wireless channel. The wireless channel situation between the user and the edge server is determined by the data transmission rate between them. Using frequency division multiple access (FDMA), according to the Shannon–Hartley theorem, the data transmission rate can be expressed as follows:

$$R = \eta B \log_2 \left(1 + \frac{Sp}{\eta B N_0} \right), \quad (3)$$

where B represents the channel bandwidth of the edge server, p represents the transmission power of the mobile device, N_0 represents the background noise, and S denotes the wireless channel gain, which is inversely proportional to distance. The proportion of the bandwidth allocated to the mobile device is denoted by η , where $\eta < 1$. Let f_s represent the computing power of the edge server, and the time taken by the edge server to compute the v_s task at time t is as follows:

$$D_s = \frac{v_s}{r} + \frac{v_s}{f_s}. \quad (4)$$

This time cost comprises two parts: the transmission time of the data and the execution time of the task on the edge server. Because the computation result of a task is often much smaller than its task size, we ignore the time required to return the computational result from the edge server to the user. The energy consumption of the mobile device uploading tasks to the edge server can be expressed as follows:

$$E_s = \frac{p v_s}{R}. \quad (5)$$

3.4. Overall Calculation Models

The total energy consumption of the user at timestamp t is the total energy consumption of the user for local task execution and task offloading to the edge server:

$$E = E_l + E_s. \quad (6)$$

The total computational latency of the user at timestamp t is the maximum value of the time spent by the user to perform a local task execution and task offloading to the edge server:

$$D = \max\{D_l, D_s\}. \quad (7)$$

This results in a total user spend of:

$$\sum_{t=1}^T C = \omega_1 E + \omega_2 D. \quad (8)$$

ω_1 and ω_2 are used as the weights for the energy consumption and computation delay, respectively. Generally speaking, the discharge of the task goal of reasonable task uninstall decisions. To minimize the total timestamp to unload T task, the total cost is

$$\begin{aligned} \min \sum_{t=1}^T C &= \omega_1 E + \omega_2 D \\ \text{s.t. } 0 &\leq r \leq 1. \end{aligned} \quad (9)$$

For this optimal model, we use a multi-branch algorithm to calculate the optimal unloading ratio, r .

3.5. Attack Models

During the task offloading process in edge computing, users tend to offload a greater number of tasks to the edge server for computation when the wireless channel quality between their mobile devices and the server is high, thereby conserving energy. Conversely, in instances of poor channel conditions, users are inclined to execute tasks locally. The state of the wireless channel is significantly correlated with the physical distance between the user and the edge server. According to the established relationship between the channel gain and distance, an increase in the distance results in a degradation of the wireless channel condition, and a decrease in distance leads to an improvement. Consequently, when the distance is reduced, the frequency of task offloading by the user increases, yielding greater benefits in terms of energy conservation and latency reduction. However, this behavior poses a risk to user privacy, which our proposed optimization method aims to mitigate by integrating differential privacy.

4. Location Privacy-Preserving Task Offloading Optimization

This chapter delves into the issue of location privacy leakage among users during the task offloading process in edge computing. When a user's objective is to minimize resource consumption through offloading, they are more likely to offload a higher volume of tasks to the edge server for computation when the wireless channel quality is high, thereby conserving energy. Conversely, under conditions of poor channel quality, the user tends to perform more tasks locally. However, the average power gain of the wireless channel is closely linked to the physical distance between the user and the edge server. Consequently, an attacker can potentially deduce the user's location by analyzing the task offloading decisions, which are reflected in the offloading ratio. We introduce an optimization method that integrates differential privacy technology to safeguard the location privacy of the user during task offloading. This method adds noise to the offloading ratio, thereby disrupting the inference of the distance between the user and edge server. We provide theoretical proof that this mechanism is effective for edge computing task offloading scenarios and satisfies the requirements of ϵ -differential privacy.

4.1. Overview of Mechanism

The paper presents a novel optimization technique for task offloading that maintains location privacy. We confronted two primary challenges: (1) preventing adversaries from discerning the user's actual task offloading decisions, thereby averting the leakage of location data; and (2) safeguarding user location privacy while concurrently minimizing the energy expenditure and computational latency inherent in the offloading process. To address these challenges, we introduce an optimization approach for task offloading that incorporates location privacy protection. Initially, the authentic offloading ratio is

ascertained based on the user's decisions and the actual distance, devoid of differential privacy. Subsequently, confusion thresholds are established based on this ratio. This strategy ensured a harmonious balance between privacy preservation and resource efficiency. The proposed task offloading optimization strategy for location privacy is divided into two components: the design of a user privacy protection mechanism and the formulation of a user task offloading mechanism. Prior to the implementation of location information privacy protection, we scrutinize the shortcomings of the traditional differential privacy methods within the task offloading context. Building on this analysis, we introduce a novel probability density function for offloading ratio obfuscation. Utilizing this function, users can obscure the offloading ratio, thereby preventing the divulgence of their location information.

4.2. Probability Density Function Design

To enhance the protection of user location privacy, this study introduces a novel probability density function designed to obfuscate the offloading ratio. This function empowers users to obscure the offloading ratio, thereby preventing the disclosure of the location information. Assuming that the true offloading ratio of users is r and the obfuscation distance is r^* , r_1 and r_2 represent the range of the upper and lower bounds of the user obfuscation distance, $\Delta r = r_2 - r_1$, and we have $r_1 < r_2$ and $r_1, r_2 \in [0, 1]$.

Differential privacy is a framework that ensures the privacy of individuals in a dataset by adding a controlled amount of noise to the data. One of the key mechanisms within this framework is the Laplace mechanism, which is particularly effective for numerical data. The Laplace distribution is chosen for its mathematical properties that align well with the requirements of differential privacy, particularly its ability to provide a controlled level of noise that ensures the indistinguishability of the output between neighboring datasets. Epsilon serves as a crucial balancing factor between privacy protection and utility of the data. It quantifies the level of indistinguishability that the mechanism ensures between the outputs of any two neighboring datasets, which differ by at most one element. A smaller epsilon value implies a higher degree of privacy protection, as it requires the mechanism to produce outputs that are very similar for similar inputs, thus making it difficult for an adversary to discern whether a particular individual's data are included in the dataset. Conversely, a larger epsilon allows for more variation in the output, potentially sacrificing some privacy for the sake of greater data utility.

With the obfuscation range in place, we then apply a differential privacy mechanism to obfuscate the offloading ratio of a user. The existing differential privacy scheme based on the Laplace mechanism is difficult to apply directly to the task offloading scenario to protect user location privacy. This paper presents a novel distance confusion probability density function, considering the constraint of the confusion range $[r_1, r_2]$. The design ensures that the total probability of the confusion offloading ratio within this range is normalized to 1. In this study, the probability density function (Pdf) that confuses offloading ratio r into ratio r^* is set as follows.

$$Pdf(r^*|r) = \begin{cases} \frac{\varepsilon}{2\Delta r} e^{-\frac{\varepsilon|r^*-r|}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2\Delta r} & \text{if } r^* \in [r_1, r_2] \\ 0 & \text{otherwise} \end{cases} \quad (10)$$

The validation of the rationality and scientific basis of this formula is detailed in Appendix A.

Consequently, once a user determines the offloading decision based on the actual distance, the actual offloading ratio becomes ambiguous. Consequently, an untrusted edge server or a potential attacker can only deduce an obscured version of the user's location from the offloading ratio. Furthermore, the randomness introduced by differential privacy for proximate datasets complicates an attacker's ability to ascertain the precise location

of the user from this obscured information. Consequently, the location data of the user remain safeguarded.

4.3. Privacy Measure Function Design

When employing a differential privacy mechanism to safeguard user location privacy, the probability that the obfuscated offloading ratio matches the user's actual offloading ratio is a critical factor. The increased likelihood of this match correlates with a higher risk of privacy leakage, whereas a lower likelihood suggests greater privacy protection. To quantify the discrepancy between the user's actual offloading ratio and the obfuscated ratio, we utilize the cross-entropy (cross-entropy loss) function. Let $Q(r)$ denote the probability distribution of the user's actual offloading ratio without differential privacy protection, and $Pdf(r^*|r)$ represent the probability distribution of the obfuscated offloading ratio under the differential privacy mechanism:

$$\int_{r_1}^{r_2} Q(r) \log Pdf(r^*|r) + (1 - Q(r)) \log(1 - Pdf(r^*|r)) dr^*. \quad (11)$$

From the definition of cross-entropy, if the value of $D(P||Q)$ is smaller, it indicates that the distribution $Pdf(r^*|r)$ fits the distribution $Q(r)$ to the distribution $Q(r)$ to a higher degree of the probability of disclosure of the proportion of the user's offloading, and privacy protection worsens the degree of privacy protection. Therefore, we set the degree of privacy leakage for a user to be the opposite of the above equation when the true offloading percentage of the user is r :

$$PL_{r_1, r_2} = - \int_{r_1}^{r_2} Q(r) \log Pdf(r^*|r) + (1 - Q(r)) \log(1 - Pdf(r^*|r)) dr^*. \quad (12)$$

5. Design of User Privacy Protection Mechanism

5.1. The Model without Privacy Protection

The goal of user task offloading at t timestamps is to make reasonable task offloading decisions (finding the local task execution ratio, $r_l(t)$, at each timestamp t) and minimize the total task offloading overhead:

$$\begin{aligned} \min \sum_{t=1}^T C &= \omega_1 E + \omega_2 D \\ s.t. 0 &\leq r \leq 1. \end{aligned} \quad (13)$$

We take the derivative of this formula and calculate different branches based on the quantitative relationship between D_l and D_s , and derive Algorithm 1 based on the relationship between each branch and the offloading ratio, r .

$$A_1 = \frac{\gamma R f_s}{\gamma R f_s + f_l f_s + R f_l}, \quad (14)$$

$$A_2 = \omega_1 k f_l \gamma + \frac{\omega_2}{f_l}, \quad (15)$$

$$A_3 = \frac{\omega_1 p}{R}, \quad (16)$$

$$A_4 = \omega_1 k f_l \gamma + \frac{\omega_2}{R} + \frac{\omega_2}{f_s}. \quad (17)$$

Algorithm 1: Optimal offloading proportion selection algorithm without privacy**Input:**

Computing power of the user's mobile device f_l
 Number of CPU cycles consumed by the mobile device to complete the task per bit γ
 User mobile device intrinsic parameters k
 Channel bandwidth for edge servers B
 Denotes the transmission power of the mobile device p
 Denotes background noise N_0
 Denotes the wireless channel gain S
 Indicates the proportion of bandwidth allocated To this mobile device η
 Denotes the computing power of the edge server f_s

Output: Unloading ratio without adding differential privacy r

1. If $A_1 > 1$
2. $r = 0$;
3. elseif $A_3 > A_2$
4. $r = 1$;
5. elseif $0 < A_1 < 1$
6. If $A_3 > A_2$
 and $A_3 > A_2 + \frac{\omega_2}{f_s}$
 $r = 0$;
7. elseif $A_3 < A_2$
 and $A_3 < A_4$
 $r = 1$;
8. elseif $A_2 < A_3 < A_4$
9. $r = 1$ when $C_1 < C_2$;
10. $r = 0$ when $C_2 < C_1$;
 elseif $A_4 < A_3 < A_2$
 $r = A_3$

5.2. Design of Optimal Confusion Range Selection Algorithm

In the previous section, we provided a new differential privacy-based noise addition to the user's offload ratio that protects the user's location privacy. However, before making task offloading decisions to determine the percentage to use for offloading, we need to determine specific values for the confusion ranges r_1 and r_2 . First, we consider the relationship between r , and r_1 and r_2 . To protect the user's location privacy while minimizing the energy consumption and computational delay during task offloading, each user in the edge computing system should adaptively add noise according to the wireless channel conditions between the user and edge server. In general, when the wireless network conditions between the user and the edge server are better (closer), the offloading ratio after obfuscation should be set to be in the high probability case; it should be larger in order to ensure that the user offloads more tasks to the edge server to save the user's resource consumption under the real location. Similarly, to ensure the utility of users making task offloading decisions based on the obfuscation ratio, r^* , over the true offloading ratio, r , we have that the utility is maximized when the obfuscation distance $r^* = r$. Therefore, it must be ensured that the confusion ratio, r^* , lies on the left and right sides of the real distance, r , similar to the value taken. Then there is the confusion range $r_1 \leq r \leq r_2$, and the closer r_1 , r_2 , and r are to the utility of task offloading decisions under the confusion distance, the better.

When the range, Δr , between r_1 and r_2 is larger, the user's privacy leakage is lower, indicating that the privacy protection mechanism proposed in this paper protects the user's location information better, and vice versa. However, when the range, Δr , between r_1 and r_2 is larger, that is, the range of the confusion interval is larger, the task offloading decision utility decreases.

Taken together, when the range, Δr , between r_1 and r_2 is narrowed, although the task offloading decision based on the obfuscation ratio can optimize the user's energy consumption and computational delay over the true distance, the degree of privacy leakage of the user's location information increases. Therefore, before performing task offloading based on the obfuscation offloading ratio, this study adaptively adjusts the lower and upper bound values of the obfuscation range based on the user's privacy protection needs and the wireless channel between the user and edge server to achieve a balance between privacy protection and task offloading utility. The formula for adjusting the lower bound value r_1 and lower bound value r_2 of the obfuscation range to balance privacy protection and task offloading utility is expressed as:

$$\omega_1 E + \omega_2 D + \omega_3 PL, \quad (18)$$

where E is the user's energy consumption, D is the user's computational delay spend cost, and ω is an influence factor that reflects the importance of the user's concern about his/her privacy leakage: the greater the user's concern about his/her privacy leakage is, the larger ω is, and, vice versa, the smaller ω is. In the most extreme case, users do not have any concern about the leakage of their location privacy. At this time, $\omega = 0$. To better adjust r_1 and r_2 , here, E and D are expected separately, and, according to Equations (6) and (7), we obtain the relationship between E and r , and D and r as follows:

$$\bar{E} = \omega(r); \bar{D} = \mu(r), \quad (19)$$

Based on the above equation, we construct the following model:

$$AM = \min \omega_1 \int_{r_1}^{r_2} \lambda(r^*) Pdf(r^*) dr^* + \omega_2 \int_{r_1}^{r_2} \mu(r^*) Pdf(r^*) dr^* + \omega_3 PL \quad (20)$$

$$s.t. \ 0 \leq r_1 \leq r \leq r_2 \leq 0.$$

The optimization objective is to minimize privacy protection and offloading utility.

For this problem, we use the simulated annealing algorithm to solve the near-optimal solution of this problem, and the specific algorithm flow is Algorithm 2.

Algorithm 2: Optimal confusion range selection algorithm

Input:

True unloading ratio without differential privacy r
 At each timestamp t , the amount of tasks generated on the user's device side m
 At each timestamp t , the wireless channel condition between the user and the server R
 Cooling rate α
 Initial temperature coefficient n
 Energy consumption factor ω_1 , latency factor ω_2 and privacy protection factor ω_3
 The law of transformation β

Output: upper and lower bounds on the integration of the unloaded proportional confusion function r_1, r_2

1. Let $r_1 = 0, r_2 = 1$.
 2. Calculate the privacy preserving and unloading utility C at this upper and lower bound, so that the initial temperature $T = nC$. The termination temperature $T_{min} = C/n$
 3. make sth. happen $r_{1new} = r - \beta(r - r_1), r_{2new} = r_2 - \beta(r_2 - r)$
 4. Calculate the utility C_{new} under new r_1, r_2
 5. If $C_{new} < C$, then accept the new solution and use r_{1new} and r_{2new} as the current solution
 6. If $C_{new} > C$, then with probability $e^{-\frac{C_{new}-C}{T}}$
 7. Let $T = \alpha * T$
 8. Repeat 3–7 and stop iterating when $T \leq T_{min}$
 9. Output the final solution r_1, r_2
-

5.3. Design of Task Offloading Optimization Algorithm for Location Privacy Protection

In the task offloading process, we first obtain the optimal offloading ratio without adding differential privacy using Algorithm 1 according to the user's current location. This initial step is crucial as it lays the foundation for subsequent privacy-enhancing measures. Following the acquisition of the optimal offloading ratio, we proceed to Algorithm 2 to calculate the upper and lower bounds of confusion, which are pivotal for the differential privacy mechanism. These bounds represent the permissible range of randomness that can be introduced to protect user privacy without significantly impairing the task execution efficiency. With the optimal bounds in hand, we then engage the offloading proportion confusion function, integrating the previously calculated upper and lower bounds to ascertain the offloading proportion post-confusion. This proportion is critical as it dictates the distribution of tasks between the local device and remote servers, taking into account the privacy-preserving confusion. Finally, Algorithm 3 elucidates the detailed procedure, guiding us through the practical application of the calculated offloading proportions to offload tasks effectively. This algorithm ensures that the theoretical calculations are translated into actionable steps, maintaining a delicate balance between efficiency and privacy throughout the task offloading process.

Algorithm 3: Task offloading optimization algorithm for location privacy protection

Input: All inputs for Algorithms 1 and 2

Output: The proportion of offloading r^* after obfuscation

1. Calculate the true offloading ratio according to Algorithm 1
 2. Calculate the optimal confusion range according to Algorithm 2
 3. Use the Pdf obfuscation function to compute the obfuscated offloading ratio r^*
-

Compared with the methods with no privacy concerns, the algorithm proposed in this study modifies the optimization objective to incorporate privacy considerations. This adjustment does not significantly increase the computational burden or complexity of the optimization algorithm, because the solving process of the optimization problem remains unchanged despite the integration of privacy into the objective function.

6. Experimental Evaluation

6.1. Simulation Parameter Setting

To better simulate the scenario of edge computing task offloading, this study selects a base station with a latitude of -37.81 and a longitude of 144.96 in the EUA dataset [35] as an edge server, and there are approximately 40 end users within its coverage. All network parameter settings are shown in Table 1. We adopt the radio communication license dataset published by the Australian Communications and Media Authority, which contains the geographical location of all cellular base stations in Australia, which are adopted as the locations of edge servers. For a user's location, the Asia Pacific Network Information Center (APNIC) provides all IP address blocks assigned to Australia, and this dataset uses the IP lookup service to translate the obtained IP addresses into geographical locations. At the same time, we simulate different scene parameters under the real dataset.

When the design of a new noise distribution is completed, it is necessary to prove that the scheme of the noise distribution satisfies the definition of differential steganography in order to guarantee the privacy-preserving performance of the mechanism.

ECORA [36]: this algorithm is named the efficient computation offloading and resource allocation algorithm (ECORA). This algorithm aims to realize the effective use of computing resources in MEC-enabled vehicular networks, reduce the delay of task completion, and improve the overall performance of the system.

Max range: users use the new probability density function proposed in this paper to confuse the offloading ratio, but do not consider the impact of the confusion range $[r_1, r_2]$ on the degree of privacy leakage and the cost of task offloading; that is, they do not choose

the confusion range $[r_1, r_2]$, and do not balance the resource cost and privacy protection, and then use the confusion offloading ratio to offload the task.

Table 1. The parameters of the MEC network.

Parameters	Values	Unit
Channel bandwidth, B	10	MHz
Background noise, N_0	−174	dBm/Hz
Path attenuation constant, g_0	−40	dB
User CPU frequency	1	GHz
Edge server CPU frequency	10	GHz
Transmission power, p	500	mw
Density of computation, γ	1000	cycle/bit
Standard distance, d_0	1	m
Computing power of the user, f_l	1	GHz
Computing power of edge servers, f_s	10	GHz

Simultaneously, we used two evaluation metrics to evaluate the effectiveness of the proposed privacy-preserving location task offloading optimization method:

Average cost: average cost refers to the T total timestamp of T in the user's average resource consumption, including the energy consumption and delay cost calculation.

Privacy leakage: privacy refers to the user in the task in the process of unloading the degree of privacy, which is expressed as PL .

By this method, considering that the user-generated task quantity has nothing to do with the equipment usage scenario, users in each set the timestamp generated task simply as $d(t) = 5$ KB. Considering the randomness caused by differential privacy, the number of tests for each point in the experiment was 1000.

6.2. Evaluation within the Model

Figure 2 illustrates the change in the proportion of users in offloading when the distance between the user and edge server changes. Figure 3 illustrates the change in the user resource cost when the distance between the user and edge server changes. Among them, the real distance between users and edge server l is within $[0, 200]$ m random values, the user privacy impact factor is 0.002, and the user privacy in the differential privacy budget is 0.1.

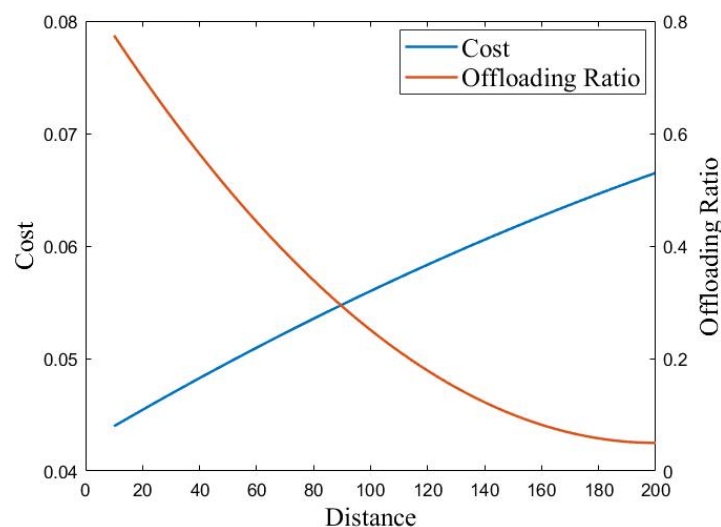


Figure 2. Relationship between distance and offloading ratio/distance and cost.

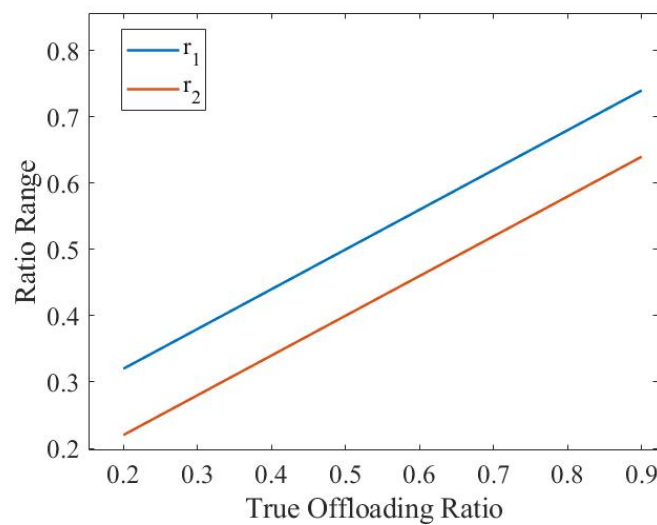


Figure 3. Relationship between true offloading ratio and ratio range.

Figure 2 demonstrates that, as the distance from the user to the edge server increases, there is a corresponding increase in the likelihood that the user will opt to process computing tasks locally, accompanied by an escalation in the user's resource consumption. This trend can be attributed to the degradation in wireless channel quality as the distance increases, which in turn diminishes the user's ability to leverage the edge server's computational resources effectively, thereby increasing reliance on local resources. Additionally, the figure shows the correlation between the user's distance from the edge server and their task offloading decisions, highlighting the importance of privacy protection during this process. By offloading tasks based on an obfuscated offloading ratio, the attacker's ability to infer the user's actual location is significantly curtailed. The incorporation of differential privacy further complicates the edge server's capacity to ascertain the user's true location from obfuscated data, thereby reinforcing the user's privacy.

Figure 3 shows that, when the proportion of user offloading increases, the difference $\Delta r = r_1 - r_2$ between the confusion interval $[r_1, r_2]$ does not change significantly. However, when the distance between the user and edge server increases, the wireless channel condition between the user and edge server will gradually deteriorate, at which point the user will perform more task processing locally, and the user's resource cost will gradually increase, as shown in Figure 2. Even though the larger and larger difference $\Delta r = r_1 - r_2$ between the confusion intervals $[r_1, r_2]$ can provide users with less privacy leakage, a larger difference in the confusion interval will increase the user's resource cost. Therefore, to better balance the relationship between user resource overhead and privacy disclosure, the confusion interval $[r_1, r_2]$ changes based on the true offloading proportion of users. That is, when the true offloading increases, the lower bound value, r_1 , and the upper bound value, r_2 , of the confusion interval both increase centered on the true offloading proportion, but the change in Δr is not obvious.

Figure 4 shows the user's different privacy impact factor, ω , and proposes the location of the unloading optimization method based on the privacy protection of the confusing range $[r_1, r_2]$ optimal value, and the resource consumption performance. The user's real unloading ratio $r = 0.5$ and the user's privacy impact factor is for 0.001, 0.002, 0.003, 0.004, and 0.005 one of these values. Figure 4 shows that, when the user privacy impact factor, ω , increases, the confusing range, as the difference between $\Delta r = r_2 - r_1$, increases because, when a user's privacy impact factor, ω , increases, the user is more concerned about privacy leaks, and they hope to have more privacy; therefore, there is less privacy leakage only when the confusing range is larger. The change trend of the upper and lower bound values of the confusion interval is different from that of Figure 3 because, in Figure 3, the real offloading ratio of users also gradually increases. To improve the effectiveness

of the mechanism proposed in this paper, the confusion interval should change with the offloading ratio (centered on the offloading ratio). Thus, there is a trend that the upper and lower bound values of the confusion interval become larger. When the true offloading ratio of the users does not change, the upper and lower bounds of the confusion interval become larger and smaller, respectively, to reduce privacy leakage. The confusion interval $[r_1, r_2]$, as the difference between the $\Delta r = r_2 - r_1$, is increasingly larger, which results in the user's resource cost also increasing gradually, as shown in Figure 5. This is because, when the confusion range is larger, users use the confusion unloading ratio to make the task of unloading decision-making utility for real, and therefore the unloading ratio becomes low. At the same time, the confusion interval increases, so that the degree of privacy leakage of the user gradually decreases. Figure 5 delineates the impact of the privacy leakage impact factor on the magnitude of privacy leakage across varying user privacy demands. Furthermore, it demonstrates the algorithm's adaptability and robustness in diverse scenarios.

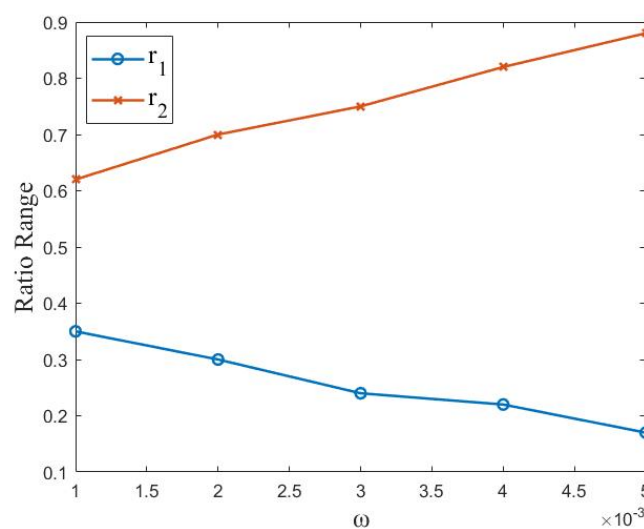


Figure 4. Relationship between privacy leakage impact factor and confusion interval.

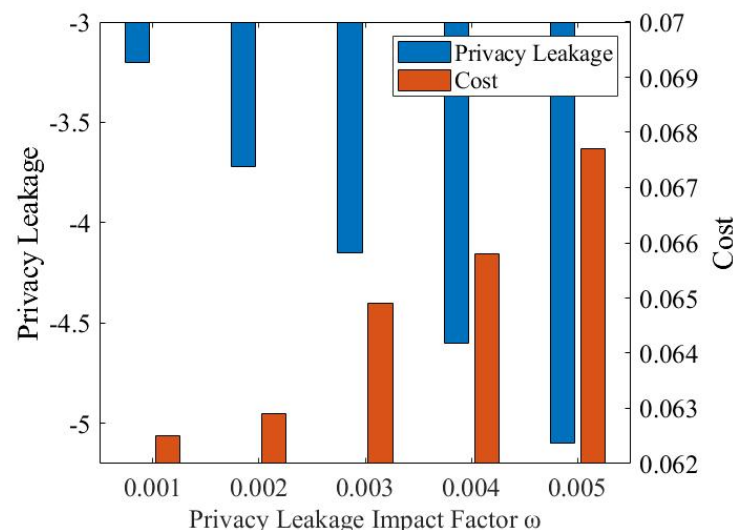


Figure 5. The relationship between privacy leakage impact factor, privacy leakage and cost.

6.3. Experimental Comparison among Models

From the data analysis in Figure 6, it can be clearly observed that, although the method we adopted is slightly higher than the theoretical value of efficiency optimization in terms of privacy leakage, its leakage risk is significantly reduced compared with the traditional

offloading method without introducing a differential privacy protection mechanism. This result demonstrates the importance and effectiveness of user privacy protection while ensuring efficiency.

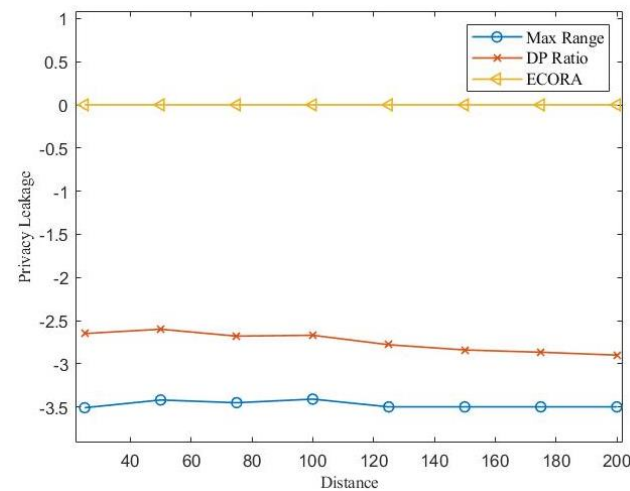


Figure 6. Relationship between distance and privacy leakage.

Figure 7 presents a comparative analysis of three distinct task offloading mechanisms, focusing on the average resource expenditure as a function of varying distances between users and edge servers. Here, “near” indicates proximity to the edge server, prompting a greater tendency of users to offload tasks. “Medium” suggests an average distance, resulting in a neutral stance towards local computation or offloading. Conversely, “far” denotes greater distances, where users prefer local computations. Regardless of distance, the proposed method, which integrates location privacy protection into task offloading optimization, exhibits a slightly higher resource cost than the ECORA method but significantly lower than the Max Range mechanism. The latter is a privacy-preserving approach that operates on a broad confusion interval based on edge server coverage. The Max Range mechanism’s broader interval, while effective for privacy, does not optimize resource costs, as task offloading decisions within this interval may not align with users’ actual location-based interests. This paper introduces an adaptive adjustment of the boundaries of the confusion range, tailored to users’ privacy needs and the quality of the wireless channel to strike a balance between privacy and offloading efficiency.

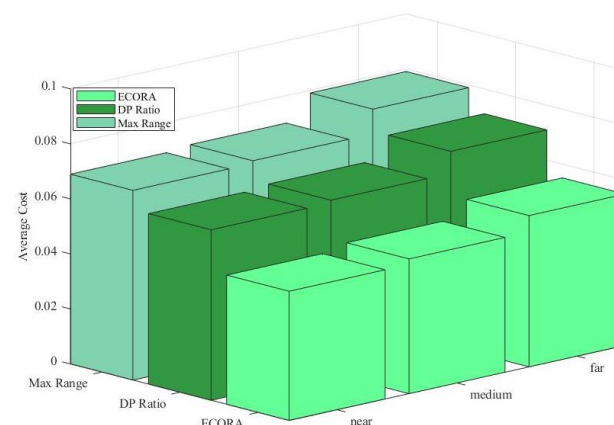


Figure 7. Relationship between distance and average cost.

7. Conclusions

This study addresses the issue of user location privacy within the context of task offloading in edge computing systems. We introduce a privacy protection method sup-

ported by rigorous theoretical proof, designed to prevent user privacy leakage while also enhancing the efficiency of user task computation. To address the challenge of location privacy leakage, we developed an optimization method for task offloading that preserves location privacy. This method enables users to dynamically set a confusion range based on fluctuating wireless channel conditions and individual privacy needs, thereby achieving a balance between privacy leakage and computational resource expenditure. Users generate a random offloading ratio within this range to inform their task offloading decisions and to safeguarding their location privacy. Our theoretical framework demonstrates the rationality and alignment of our location privacy protection method by using differential privacy principles. Moreover, the experimental results indicate that our method effectively balances the trade-off between user privacy and resource costs, thereby maximizing user benefits during the task offloading process in edge computing. Furthermore, our methodology is extensible to various domains, including the Internet of Vehicles, location-based services, mobile crowdsourcing, and industrial manufacturing, with a focus on safeguarding user privacy. Nonetheless, the current model is confined to scenarios involving multiple users and a single server, omitting the scenarios with multi-users and multi-servers. In addition, comprehensive analyses of the performance of solutions is required as the scale of users and tasks increases. This will be a pivotal aspect of our future research endeavors, ensuring that our mechanism is robust and adaptable to varying scales of deployment.

Author Contributions: Conceptualization, G.Z.; methodology, G.Z. and S.Z.; software, Z.M.; validation, Z.M., C.C. and W.H.; investigation, S.Z.; resources, G.Z.; writing—original draft preparation, G.Z.; writing—review and editing, S.Z.; visualization, C.C. and W.H.; supervision, G.Z.; project administration, G.Z.; funding acquisition, G.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Shandong Province grant number ZR2021QF090.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is contained within the article.

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

Appendix A

Appendix A.1

For the proposed task offloading optimized noise probability density (PDF function) for location privacy preservation, the total probability is 1 in the confusion range $[r_1, r_2]$.

For the probability density function based on the proportion of confusion offloading proposed in this paper (10), we integrate the confusion range $[r_1, r_2]$ and calculate the total probability of the confusion range $[r_1, r_2]$:

$$\begin{aligned}
 & \int_{r_1}^{r_2} \frac{\varepsilon}{2\Delta r} e^{-\frac{\varepsilon|r^*-r|}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2\Delta r} dr^* \\
 &= \int_{r_1}^r \frac{\varepsilon}{2\Delta r} e^{-\frac{\varepsilon(r^*-r)}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} dr^* + \int_r^{r_2} \frac{\varepsilon}{2\Delta r} e^{-\frac{\varepsilon(r^*-r)}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} dr^* \\
 &= \frac{1}{2} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r - \frac{1}{2} e^{\frac{\varepsilon(r_1-r)}{\Delta r}} \\
 &= \frac{1}{2} e^{\frac{\varepsilon(r^*-r)}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r^* \Big|_{r_1}^r + \left(-\frac{1}{2} e^{-\frac{\varepsilon(r^*-r)}{\Delta r}} + \frac{e^{\frac{\varepsilon(r_1-r)}{\Delta r}} + e^{-\frac{\varepsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r^* \right) \Big|_r^{r_2}
 \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2} + \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r - \frac{1}{2} e^{\frac{\epsilon(r_1-r)}{\Delta r}} - \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r_1 - \frac{1}{2} e^{-\frac{\epsilon(r_2-r)}{\Delta r}} \\
&\quad + \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r_2 + \frac{1}{2} - \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{2(r_2-r_1)} \cdot r = 1
\end{aligned}$$

After proving that the total probability is 1 in the confusion range $[r_1, r_2]$, the offloading ratio of users will not be confused to the region beyond $[r_1, r_2]$, demonstrating the reasonableness of the new probability density function proposed in this paper.

Appendix A.2

For a user's true offloading ratio, r , and its neighborhood distance, r' , we prove that, after applying the location privacy-preserving task offloading optimization method proposed in this paper, the ratio between the probability of confusion from the true offloading ratio, r , to r' , $Pdf(r^*|r)$, and the probability of confusion from the neighborhood offloading ratio, r , to r' , $Pdf(r^*|r')$, satisfies the definition of ϵ -differential privacy.

$$\begin{aligned}
\frac{Pdf(r^*|r)}{Pdf(r^*|r')} &= \frac{\frac{\epsilon}{2\Delta r} e^{-\frac{\epsilon|r^*-r|}{\Delta r}} + \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{2\Delta r}}{\frac{\epsilon}{2\Delta r} e^{-\frac{\epsilon|r^*-r'|}{\Delta r}} + \frac{e^{\frac{\epsilon(r_1-r')}{\Delta r}} + e^{-\frac{\epsilon(r_2-r')}{\Delta r}}}{2\Delta r}} = \frac{e^{-\frac{\epsilon|r^*-r|}{\Delta r}} + \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{\epsilon}}{e^{-\frac{\epsilon|r^*-r'|}{\Delta r}} + \frac{e^{\frac{\epsilon(r_1-r')}{\Delta r}} + e^{-\frac{\epsilon(r_2-r')}{\Delta r}}}{\epsilon}} \\
&\leq \max \left(\frac{e^{-\frac{\epsilon|r^*-r|}{\Delta r}}}{e^{-\frac{\epsilon|r^*-r'|}{\Delta r}}}, \frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}} + e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{e^{\frac{\epsilon(r_1-r')}{\Delta r}} + e^{-\frac{\epsilon(r_2-r')}{\Delta r}}} \right) \leq \max \left(e^{-\frac{\epsilon|r'-r|}{\Delta r}}, \max \left(\frac{e^{\frac{\epsilon(r_1-r)}{\Delta r}}}{e^{\frac{\epsilon(r_1-r')}{\Delta r}}}, \frac{e^{-\frac{\epsilon(r_2-r)}{\Delta r}}}{e^{-\frac{\epsilon(r_2-r')}{\Delta r}}} \right) \right) \\
&\leq \max(e^\epsilon, \max(e^\epsilon, e^\epsilon)) = e^\epsilon
\end{aligned}$$

The above proofs show that the task offloading optimization for location privacy preservation proposed in this paper satisfies the definition of ϵ -differential privacy, and the method has rigorous privacy-preserving theoretical proof.

References

1. Arun, V.; Azhagiri, M. Design of Long-Term Evolution Based Mobile Edge Computing Systems to Improve 5G Systems. In Proceedings of the Second International Conference on Edge Computing and Applications, Coimbatore, India, 20–21 March 2023; Volume 979–83503–47579.
2. Mouha, R.A. Internet of Things (IoT). *J. Data Anal. Inf. Process.* **2021**, *9*, 77–101.
3. Wang, Y.; Zhao, S. Research on Fine-Grained Task Offloading in Mobile Edge Computing. In Proceedings of the 2023 4th International Conference on Information Science, Parallel and Distributed Systems (ISPDS), Guangzhou, China, 14–16 July 2023; pp. 526–529.
4. Lu, G.; Zhang, W.; Liu, M.; Hou, R.; Gao, L. Construction of Edge Computing Cloud Service Platform Based on BP Neural Network. In Proceedings of the 2023 International Conference on Networking, Informatics and Computing (ICNETIC), Palermo, Italy, 29–31 May 2023; pp. 487–491.
5. Zhang, R.; Zhou, C. A Computation Task Offloading Scheme based on Mobile-Cloud and Edge Computing for WBANs. In Proceedings of the ICC 2022—IEEE International Conference on Communications, Seoul, Republic of Korea, 16–20 May 2022; pp. 4504–4509.
6. Leo, L.M.; Yogalakshmi, S.; Veeramuthu, A.; Kalist, V.; Joe, A.A.F. Experimental Analysis of Data Storage and Integrity Management over Cloud Environment using Integrated Data Security Strategy. In Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 16–18 March 2022; pp. 952–957.
7. Hensh, F.; Gupta, M.; Nene, M.J. Mist-Edge-Cloud (MEC) Computing: An Integrated Computing Architecture. In Proceedings of the 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 4–6 August 2021; pp. 1035–1040.
8. Ding, N.; Liu, Y.; Farokhi, F. A Linear Reduction Method for Local Differential Privacy and Log-lift. In Proceedings of the 2021 IEEE International Symposium on Information Theory (ISIT), Virtual Event, 12–20 July 2021.

9. Zhang, P.; Wang, C.; Aujla, G.S.; Batth, R.S. ReLeDP: Reinforcement-Learning-Assisted Dynamic Pricing for Wireless Smart Grid. *IEEE Wirel. Commun.* **2021**, *28*, 62–69. [\[CrossRef\]](#)
10. Wang, C.; Yuan, Z.; Zhou, P.; Xu, Z.; Li, R.; Wu, D.O. The Security and Privacy of Mobile-Edge Computing: An Artificial Intelligence Perspective. *IEEE Internet Things J.* **2023**, *10*, 22008–22032. [\[CrossRef\]](#)
11. Pusti, B.; Sankaran, S. Security and Energy-Aware Resource Allocation in Mobile Edge Computing (MEC). In Proceedings of the 2022 IEEE International Symposium on Smart Electronic Systems (iSES), Warangal, India, 19–21 December 2022; pp. 293–296.
12. Radouane, B.; Lyamine, G.; Ahmed, K.; Kamel, B. Scalable Mobile Computing: From Cloud Computing to Mobile Edge Computing. In Proceedings of the 2022 5th International Conference on Networking, Information Systems and Security: Envisage Intelligent Systems in 5g / 6G-based Interconnected Digital Worlds (NISS), Bandung, Indonesia, 30–31 March 2022; pp. 1–6.
13. Liu, L.; Feng, J.; Mu, X.; Pei, Q.; Lan, D.; Xiao, M. Asynchronous Deep Reinforcement Learning for Collaborative Task Computing and On-Demand Resource Allocation in Vehicular Edge Computing. *IEEE Trans. Intell. Transp. Syst.* **2022**, *24*, 15513–15526. [\[CrossRef\]](#)
14. Mei, J.; Tong, Z.; Li, K.; Zhang, L.; Li, K. Energy-Efficient Heuristic Computation Offloading With Delay Constraints in Mobile Edge Computing. *IEEE Trans. Serv. Comput.* **2023**, *16*, 4404–4417. [\[CrossRef\]](#)
15. Li, J.; Liang, W.; Xu, W.; Xu, Z.; Jia, X.; Zhou, W.; Zhao, J. Maximizing User Service Satisfaction for Delay-Sensitive IoT Applications in Edge Computing. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *33*, 1199–1212. [\[CrossRef\]](#)
16. Sun, J.; Gu, Q.; Zheng, T.; Dong, P.; Valera, A.; Qin, Y. Joint Optimization of Computation Offloading and Task Scheduling in Vehicular Edge Computing Networks. *IEEE Access* **2020**, *8*, 10466–10477. [\[CrossRef\]](#)
17. Zeng, Y.; Liu, D. Computation Offloading Based on Improved Sparrow Search Algorithm in Edge Computing Scenario. In Proceedings of the 2022 International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT), Xiamen, China, 28–30 October 2022; pp. 231–236.
18. Wang, L.; Deng, X.; Gui, J.; Zhang, H.; Yu, S. Computation Placement Orchestrator for Mobile-Edge Computing in Heterogeneous Vehicular Networks. *IEEE Internet Things J.* **2023**, *10*, 22686–22702. [\[CrossRef\]](#)
19. Zhuo, Z.; Dong, S.; Zheng, H.; Zhang, Y. Method of Minimizing Energy Consumption for RIS Assisted UAV Mobile Edge Computing System. *IEEE Access* **2024**, *12*, 39678–39688. [\[CrossRef\]](#)
20. Zakarya, M.; Gillam, L.; Ali, H.; Rahman, I.U.; Salah, K.; Khan, R.; Rana, O.; Buyya, R. epcAware: A Game-Based, Energy, Performance and Cost-Efficient Resource Management Technique for Multi-Access Edge Computing. *IEEE Trans. Serv. Comput.* **2022**, *15*, 1634–1648. [\[CrossRef\]](#)
21. Khazali, A. Joint Task Assignment, Power Allocation and Node Grouping for Cooperative Computing in NOMA-mmWave Mobile Edge Computing. *IEEE Access* **2023**, *11*, 93664–93678. [\[CrossRef\]](#)
22. Shinde, S.S.; Bozorgchenani, A.; Tarchi, D.; Ni, Q. On the Design of Federated Learning in Latency and Energy Constrained Computation Offloading Operations in Vehicular Edge Computing Systems. *IEEE Trans. Veh. Technol.* **2022**, *71*, 2041–2057. [\[CrossRef\]](#)
23. Wang, L.; Zhang, G. Joint Service Caching, Resource Allocation and Computation Offloading in Three-Tier Cooperative Mobile Edge Computing System. *IEEE Trans. Netw. Sci. Eng.* **2023**, *10*, 3343–3353. [\[CrossRef\]](#)
24. Samir, R.; El-Hennawy, H.; El-Badawy, H.M. Orchestration of MEC Computation Jobs and Energy Consumption Challenges in 5G and Beyond. *IEEE Access* **2022**, *10*, 18645–18652. [\[CrossRef\]](#)
25. Qin, Z.; Ye, J.; Meng, J.; Lu, B.; Wang, L. Privacy-Preserving Blockchain-Based Federated Learning for Marine Internet of Things. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 159–173. [\[CrossRef\]](#)
26. Asheralieva, A.; Niyato, D.; Xiong, Z. Auction-and-Learning Based Lagrange Coded Computing Model for Privacy-Preserving, Secure, and Resilient Mobile Edge Computing. *IEEE Trans. Mob. Comput.* **2023**, *22*, 744–764. [\[CrossRef\]](#)
27. Liu, T.; Di, B.; An, P.; Song, L. Privacy-Preserving Incentive Mechanism Design for Federated Cloud-Edge Learning. *IEEE Trans. Netw. Sci. Eng.* **2021**, *8*, 2588–2600. [\[CrossRef\]](#)
28. Wang, H.; Fan, K.; Zhang, K.; Wang, Z.; Li, H.; Yang, Y. Secure and Efficient Data-Privacy-Preserving Scheme for Mobile Cyber-Physical Systems. *IEEE Internet Things J.* **2022**, *9*, 22375–22388. [\[CrossRef\]](#)
29. Cao, B.; Li, Z.; Liu, X.; Lv, Z. Privacy-Preserving Task Offloading in Vehicular Edge Computing, in Privacy-Preserving Scheme for Mobile Cyber-Physical Systems. In Proceedings of the 2023 Asia Symposium on Image Processing (ASIP), Tianjin, China, 15–17 June 2023; pp. 156–160.
30. Wang, Z.; Sun, Y.; Liu, D.; Hu, J.; Pang, X.; Hu, Y.; Ren, K. Location Privacy-Aware Task Offloading in Mobile Edge Computing. *IEEE Trans. Mob. Comput.* **2024**, *23*, 2269–2283. [\[CrossRef\]](#)
31. Zhang, S.; Hu, B.; Liang, W.; Li, K.-C.; Gupta, B.B. A Caching-Based Dual K-Anonymous Location Privacy-Preserving Scheme for Edge Computing. *IEEE Internet Things J.* **2023**, *10*, 9768–9781. [\[CrossRef\]](#)
32. Du, J.; Zhang, G.; Yuan, X.; Zang, X. P²SPA: Privacy Preservation Strategy with Pseudo-Addresses for Edge Computing Networks. *IEEE Access* **2024**, *12*, 40962–40972. [\[CrossRef\]](#)
33. Yao, A.; Pal, S.; Dong, C.; Li, X.; Liu, X. A Framework for User Biometric Privacy Protection in UAV Delivery Systems with Edge Computing. In Proceedings of the 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Biarritz, France, 11–15 March 2024; pp. 631–636.
34. Jiang, B.; Li, J.; Wang, H.; Song, H. Privacy-Preserving Federated Learning for Industrial Edge Computing via Hybrid Differential Privacy and Adaptive Compression. *IEEE Trans. Ind. Informatics* **2023**, *19*, 1136–1144. [\[CrossRef\]](#)

35. EUA Datasets. Available online: <https://github.com/PhuLai/eua-dataset> (accessed on 2 March 2024).
36. Li, Y.; Li, L. Computation Offloading and Resource Allocation in MEC-enabled Vehicular Networks: Partial Offloading Versus Binary Offloading. In Proceedings of the 2024 7th World Conference on Computing and Communication Technologies (WCCCT), Chengdu, China, 12–14 April 2024; pp. 260–266.

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.