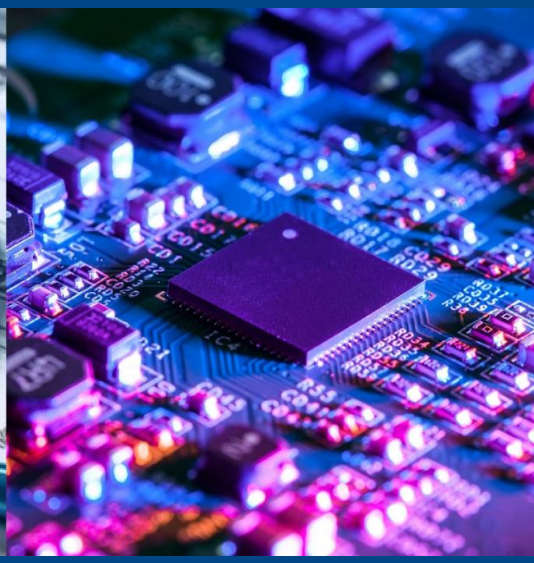
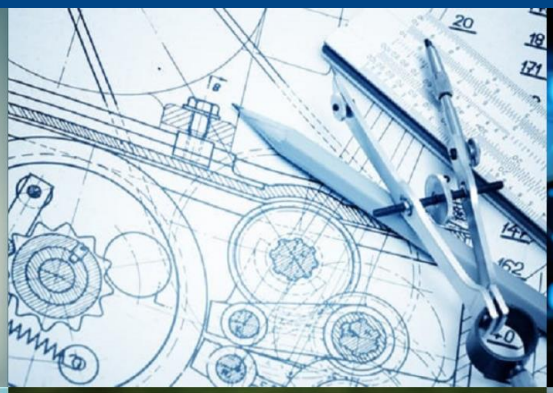
ISSN: 2582-7219

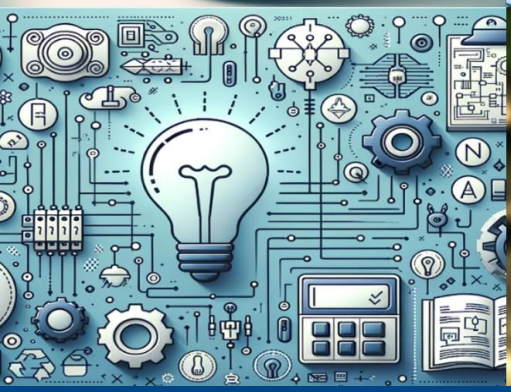




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 8, Issue 3, March 2025**

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803249

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Protecting Location Privacy During Task Allocation in Mobile Cloud Computing

Dr. D.J. Samatha Naidu, K. Venkata Ramya, K. Kalyan

Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

Assistant Professor, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

PG Student, Dept. of MCA, APGCCS, New Boyanapalli, Rajampet, A.P, India

ABSTRACT: Mobile cloud computing is an emerging cloud computing paradigm that integrates cloud computing and mobile computing to enable many useful mobile applications. However, the large-scale deployment of mobile cloud computing is hindered by the concerns on possible privacy leakage. In this project, I investigate the privacy issues in the ad hoc mobile cloud computing, and propose a framework that can protect the location privacy when allocating tasks to mobile devices. My mechanism is based on differential privacy and geocast and allows mobile devices to contribute their resources to the ad hoc mobile cloud without leaking their location information. I develop analytical models and task allocation strategies that balance privacy, utility, and system overhead in an ad hoc mobile cloud. I also conduct extensive experiments based on real-world datasets, and the results show that our framework can protect location privacy for mobile devices while providing effective services with low system overhead.

KEYWORDS: Location Privacy, Task Allocation, Mobile Cloud Computing, Privacy-Preserving Task Offloading

I. INTRODUCTION

Nowadays, mobile devices such as smartphones and tablets have gained tremendous popularity. These devices are often equipped with a variety of sensors such as camera, microphone, GPS, accelerometer, gyroscope, and compass. The data (e.g., position, speed, temperature, and heart rate) generated by these sensors enable many useful mobile applications, including location-based services, mobile sensing and mobile crowdsourcing. Although improved largely over the past several years, mobile devices are still resource-constrained mainly due to the limited battery lifetime. On the other hand, cloud computing has widely been regarded as the next-generation computing paradigm which provides “unlimited” cloud resources to end-users in an on-demand fashion. The rich cloud resources in cloud computing can be exploited to increase, enhance, and optimize capabilities of mobile devices, leading to the concept of mobile cloud computing (MCC). According to, MCC integrates cloud computing technologies with mobile devices to make the mobile devices more capable in terms of computational power, memory, storage, energy, and context awareness. There are generally two types of mobile clouds in MCC: infrastructure-based and ad hoc. The infrastructure-based mobile cloud consists of stationary computing resources and provides services to the mobile users via the Internet. Alternatively, in the ad hoc mobile cloud, a collection of mobile devices (hereafter referred to as “mobile servers”) performs as cloud resources and provides access to local or Internet-based cloud services to other mobile users (hereafter referred to as “mobile clients”). In this paper, we focus on the second case, namely, the ad hoc mobile cloud. The main benefit of utilizing ad hoc mobile cloud resources is their distributed and features. Finally, there is an inherent conflict between quality of service (i.e., utility) and privacy in task allocation. If an ad hoc mobile cloud ensures privacy of mobile servers, it is difficult to guarantee the utility of their MCC service. Finding a solution that ensures privacy while guaranteeing utility for task allocation is a major challenge in such systems. Several solutions to privacy issues in mobile applications have been proposed. For example, aggregation is a common approach to hiding individual sensitive information when only statistics of users are required. However, this approach only calculates statistics and thus cannot be used to select mobile servers in an ad hoc mobile cloud.

II. SYSTEM MODEL AND ASSUMPTIONS

Mobile users generate computational tasks and request cloud services while aiming to keep their locations private. Each user device is equipped with privacy-preserving mechanisms, such as encryption and obfuscation techniques, to prevent

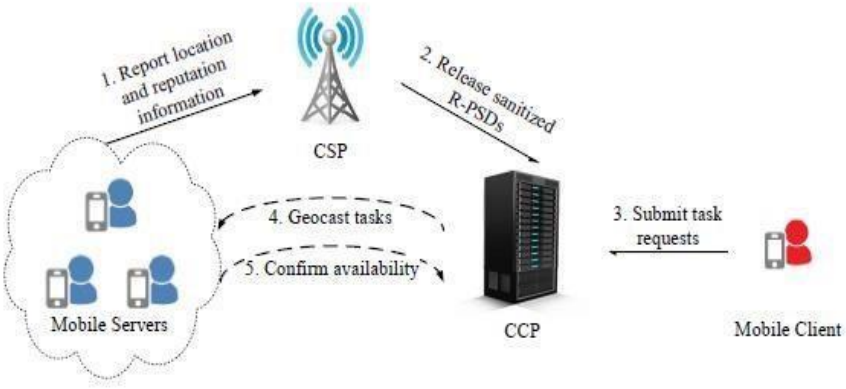
© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803249

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

direct exposure of their real-time location. The users interact with the system by submitting task requests without revealing precise geographic details.Cloud service providers (CSPs) handle computational tasks and allocate resources efficiently. They process encrypted or obfuscated location data without requiring precise user locations. The CSPs use privacy-aware task scheduling algorithms, such as federated learning or secure multi-party computation (SMPC), to ensure optimal task allocation without compromising user anonymity.



III. EFFICIENT COMMUNICATION

Mobile Cloud Computing (MCC) enhances the capabilities of mobile devices by offloading tasks to cloud servers. However, task allocation in MCC raises significant privacy concerns, particularly regarding users' location data. Adversaries can exploit this data for tracking, profiling, or unauthorized access. Various strategies, including cryptographic methods, anonymization, and differential privacy, have been proposed to address these concerns.

1. Location Tracking

- Attackers can infer users' real-time or historical locations based on task allocation requests. Studies highlight vulnerabilities where an adversary, by observing task allocation patterns, can reconstruct user mobility trajectories.
- Task requests often contain implicit location information, which can be intercepted and exploited. Research has demonstrated that adversaries can correlate these requests with external datasets to pinpoint user locations.

2. Location Anonymization Techniques

- K-Anonymity: Ensures that a user's location is indistinguishable from at least other users. Research has extended this concept to MCC by grouping similar task requests.
- Mix-Zones: Users frequently change pseudonyms in specific areas to prevent tracking. This technique has been adapted to task allocation models to obfuscate location traces.
- Dummy Location Generation: Users send multiple fake locations along with their real location to obscure their actual position.

3. Differential Privacy-Based Methods

- Noise Addition:Techniques like Laplace or Gaussian noise are added to location data to prevent exact identification.
- Task Allocation with Perturbed Locations: Studies integrate differential privacy into MCC task allocation models to ensure privacy while preserving utility.

IV. SECURITY

In mobile cloud computing (MCC), protecting location privacy during task allocation is crucial to prevent unauthorized tracking and potential security threats. To address this, we propose a privacy-preserving task allocation model that ensures minimal exposure of users' locations while optimizing resource utilization. Our model leverages obfuscation techniques, cryptographic methods, and decentralized computing frameworks to enhance privacy and efficiency. In this module, the service provider will browse the data file, initialize the router nodes and then send to the particular receivers. Service

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803249

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

provider will send their data file to router and router will select smallest distance path and send to particular receiver. The Router manages a Multiple Networks provide data storage service. In network n-number of nodes are present (n1, n2, n3, n4, n5…). In a router service provider can view node details and attacked nodes. Service provider will send their data file to router and router will select single path and any path with distance calculation and send to particular receiver. If any attacker is found in a Node then router will connect to another node and send to particular user.

V. RESULT AND DISCUSSION

In the fig 1, In above screen after completion of source file execution again open the "Cloud Server.java" file and run the code to execute the out file displays on the screen.

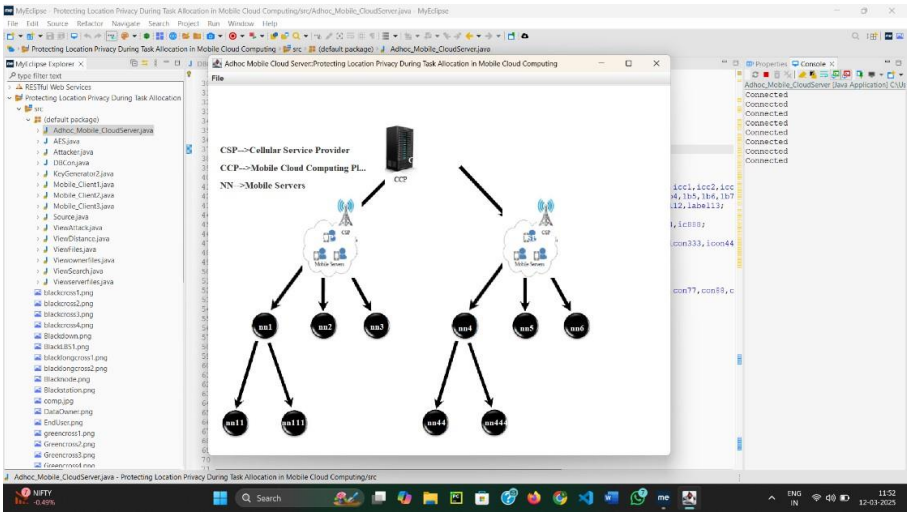


Fig. 1 Cloud Server

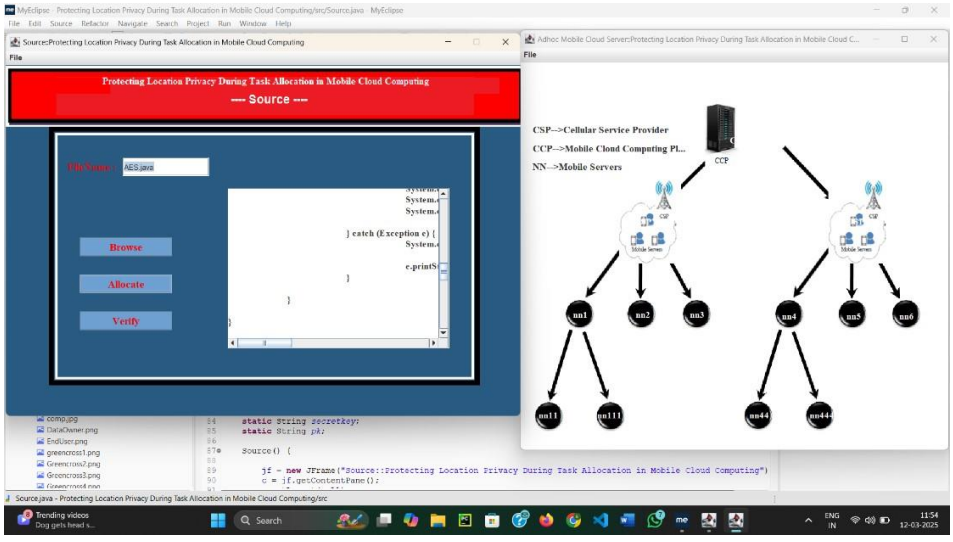


Fig. 2 Allocate

In the fig 2, This screen involves the cloud server handling file allocation. The cloud server is responsible for managing and distributing files among clients or nodes

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803249

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

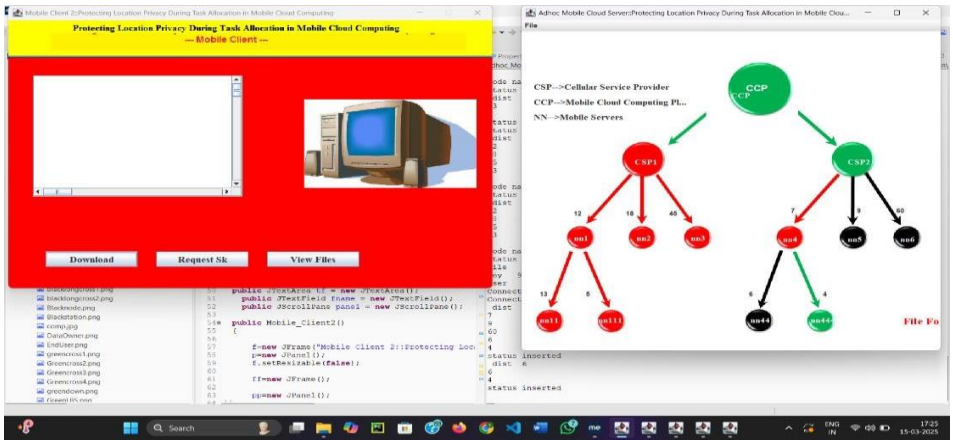


Fig .3 Client2 BS checking node

In Fig 3, The color-coded nodes (green and red) might indicate trusted vs. untrusted nodes or different levels of access control.

VI. CONCLUSION

To the best of our knowledge, this paper is the first study about optimal encoding parameters for representation sets in free-viewpoint adaptive streaming. We have defined an optimization problem for the selection of the representation set that maximizes the average satisfaction of interactive users while minimizing their view switching delay. We define a novel variable, namely the multi-view navigation segment, and formulate an optimization problem that can be solved as a tractable ILP problem. We characterize the satisfaction of interactive users as the quality experienced by the user during the navigation. This function is able to take into account both coding and view synthesis artifacts. We finally measure the performance of representation sets based on content provider recommendations and show the suboptimality of baseline algorithms that do not adapt the coding parameters to the video and users characteristics We therefore highlight the gap between existing recommendations and solutions that maximize the average user satisfaction. In particular, we show that an unequal allocation of the storage capacity among different video types as well as camera views is essential to strike for the right balance between storage cost and users satisfaction in interactive multi-view video systems

REFERENCES

[1] T. Spyropoulos, R. Rais, T. Turletti, K. Obraczka, and A. Vasilakos, “Routing for disruption tolerant networks: taxonomy and design,” Wireless Networks, vol. 16, no. 8, pp. 2349–2370, 2010.
[2] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, “Trust management for encounter-based routing in delay tolerant networks,” in IEEE Global Telecommunications Conference, Miami, FL, 6-10 Dec. 2010, pp. 1–6.
[3] “Dynamic trust management for delay tolerant networks and its application to secure routing,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 5, pp. 1200–1210, May 2014.
[4] P. Buneman, S. Khanna, and W. Tan, “Why and where: A characterization of data provenance,” in Proceedings of International Conference on Database Theory, Springer-Verlag, 2001, pp. 316–330.
[5] F. Safaei, P. Boustead, C. D. Nguyen, J. Brun, and M. Dowlatshahi, “Latency-driven distribution: Infrastructure needs of participatory entertainment applications,” IEEE Commun. Mag., vol. 43, no. 5, pp. 106–112, May 2005.
[6] M. Mauve, J. Vogel, V. Hilt, and W. Effelsberg, “Local-lag and timewarp: Providing consistency for replicated continuous applications,” IEEE Trans. Multimedia, vol. 6, no. 1, pp. 47–57, Feb. 2004.
[7] V. Valancius, N. Laoutaris, L. Massoulie_, C. Diot, and P. Rodriguez, “Greening the internet with nano data centers,” in Proc. ACM 5th Int. Conf. Emerging Netw. Exp. Technol., 2009, pp. 37–48.
[8] S. Choy, B. Wong, G. Simon, and C. Rosenberg, “The brewing storm in cloud gaming: A measurement study on cloud to enduser latency,” in Proc. ACM 11th Annu. Workshop Netw. Syst. Support Games, 2012, pp. 1–6.
[9] D. Delaney, T. Ward, and S. McLoone, “On consistency and network latency in distributed interactive applications: A surveypart i,” Presence: Teleoperators Virtual Envir., vol. 15, no. 2, pp. 218– 234, 2006.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com