A LOCATION PRIVACY PROTECTING TECHNIQUE FOR RESOURCE ENHANCEMENT IN MOBILE CLOUD SYSTEM

Dr V.M. Thakare¹, Dr S.S. Sherekar², N.L. Rathod

1Head of Department, PG Department of Computer Science, SGBAU Amravati, India.
2 Professor, PG Department of Computer Science, SGBAU Amravati, India.
3 Student, ME (CSIT), PG Department of Computer Science, SGBAU Amravati, India.

ABSTRACT

Location privacy to resources in resource allocation mechanism is main issue in mobile cloud computing. Many researches have been worked for providing location privacy to cloud resources. Challenges of MCC are heterogeneity in wireless networks like, limited device and storage memory multiple operating systems, multiple network interfaces etc. This paper proposes a security mechanism called as cloud masking. The main idea of the masking technique is to present data differently to servers to preserve user's privacy. Thus providing cloud resources with location privacy is the main focused area for the work presented here. This can be achieved using cloud masking technique.

Keywords—Data allocation, location Privacy, mobile cloud computing, resource allocation.

1. INTRODUCTION

As more mobile devices are available today lots of resources are accessible. This devices suffers from problems like battery lifetime, limited processor power, so computation offloading is the main task to shorten processing time. Many offloading schemes are used over recent years. Linear programming using task graph is method used for improving computation power of devices [1]. Mobile cloud computing involves lots of devices which are equipped with sensors such as camera, microphone etc. data or information is transfer from one device to another so there is chance of data leakage or privacy leakage. Several solutions are proposed to solve privacy issues. Aggregation is a method used for hiding sensitive information. Where only user statistic is required [2]. Cloudlet to cloudlet resource extensionin which cloudlet collaboration is done for allocation of tasks to a group of cloudlets in efficient manner is given. Cloudlet resources can be extended using clouds where less time sensitive computations can be shifted to cloud while time critical execution is done in the cloudlet [3].Hybrid memory architectures for processor cores and cache systems design have drawn much attention recently. A heuristic algorithm which works on global variables, stack variables, and program code is given [4]. Several algorithms are designed to determine whether to offload current task, in cloudlet or compute locally. A Lyapunov optimization-based dynamic computation offloading algorithm is introduced to maximize the long term average revenue of a MD. A data offloading decision algorithm is used to let MD to choose whether it should offload the tasks to a remote cloud, a cloudlet or an Ad-hoc MCC [5].

This paper introduces different resource allocation strategies with security to resources by utilizing system memory for processing such as Time allocation scheme algorithm (TAS), Privacy based model, Mobile device

based cloudlet model, dynamic data allocation model, dynamic resource allocation model. These models gives better outcome but some limitations are still there which are overcome by cloud masking technique which mainly used for providing security so that privacy is maintained.

2. BACKGROUND

Many studies are being done for security of cloud resources for maintaining privacy among different users using data and resources dynamically. This paper not only gives security to resources but also provides resources in efficient manner so that resources are utilize optimally using different memory architectures. Time allocation scheme is algorithm in which application task graph are shown by serial trees where each node and edge has given a number.A node specifies a computing task labelled with its workload and an edge implies data dependency labelled with the amount of data transmission. At application run time, acknowledgement is sent upon task completion and data reception. The leader takes care of node failure when acknowledge timeouts [1].Privacy based model provides a framework that can achieve differential privacy for mobile server location data while providing high service quality. This model gives reputation score of mobile server so a mobile server with a high reputation indicates that it has been providing reliable results for past tasks [2]. Mobile device based cloudlet model is proposed for resources that can used only its own tasks, ensuring privacy and integrity of the users. As this model comprises of cloudlet the computational overhead is reduce .If cloudlet is overloaded then each mobile device performs its offloaded task [3].Dynamic data allocation model is the first model which can efficiently allocate data on each memory unit in polynomial time. This paper is proposed for overcoming resource scheduling problem due to low memory access performance [4]. Dynamic resource allocation model is proposed for Ad-hoc MCC, in which resources are provided when infrastructure is not available [5].

This paper introduces resource allocation schemes along with privacy preservation schemes i.e.as Time allocation scheme algorithm (TAS), Privacy based model, Mobile device based cloudlet model, dynamic data allocation model, dynamic resource allocation model. These are organized as follows:

Section I Introduction. Section II discusses Background. Section III discusses previous work. Section IV discusses existing methodologies. Section V discusses Analysis and discussion Section VI present Overview of cloud masking technique for location privacy of resources. Its outcome possible results are analyzed in Section VII. Section VIII concludes this paper. Finally Section IX presents future scope.

3. PREVIOUS WORK DONE

Yi Hsuan Kao et al. (2017) [1] has proposed a time allocation scheme algorithm for minimizing the application latency while meeting the prescribed resource utilization constraints. Yanmin Gong et al. (2015) [2] has proposed a privacy maintaining frameworks for protecting cloud privacy.Cloud contains different resources at many places for users so it is typical that privacy may be leaked, this model work on preserving privacy.MdWhaiduzzaman et al. (2016) [3] has proposed mobile device based cloudlet model. In which each mobile device acts as cloudlet whenever cloudlet is overloaded. So this mobile devices offload its own task.MeikangQiu et al. (2017) [4] has proposed a dynamic data allocation scheme as name suggest data allocated to memory dynamically, this scheme is mostly useful for memory utilization in cloud systems.Weiwei Chen et al. (2017) [5] has proposed a dynamic resource allocation scheme, this scheme is useful for allocating

resources dynamically. It works on Task graph basis in which each device is called as node, and each node communicate with each other by D2D techniques.

4. EXISTING METHODOLOGIES

Many resource allocation strategies are designed and implemented over years. There are different methodologies which are implemented for different resource allocation schemes i.e. Time allocation Scheme (TAS), Privacy based framework, mobile device based cloudlet model, dynamic data allocation scheme, dynamic resource allocation scheme.

4.1 TIME ALLOCATION SCHEME

Time allocation scheme is concerned with task assignment problem, task dependency is taken into consideration [1]. TAS aims is to minimize the latency subject to cost constraint. It is a fully polynomial time approximation scheme (FPTAS). For all instances, it always outputs a solution that gives no more than(1+E) times of the minimum objective, where E is a positive number, and the complexity is bounded by a polynomial in 1/E and the problem size, identify for a subset of problem instances, where the application task graphs can be described as serial trees, admits a (1+E) approximation and runs in O(dinNM2 1/E log 2T) time ,where N is the number of tasks ,M is the number of devices, din is the maximum in degree over all tasks ,l is the length of the longest paths and T is the dynamic range. A node specifies a computing task labelled with its workload and an edge implies data dependency labelled with the amount of data transmission. At application run time, acknowledgement is sent upon task completion and data reception. The leader takes care of node failure when acknowledge timeouts.



Fig.4.1 Task Graph in TAS

4.2 PRIVACY BASED FRAMEWORK

Privacy based framework considers both location privacy of cloud resources as well as service quality. Four main components of this system are mobile servers, Cellular service provider (CSP), cloud computing platform (CCP), mobile client. This system works as follows:

Step 1

First of all, mobile servers send their locations, and reputation scores to the CSP.

Step 2

Who then collects updates and releases a Reputation-based Private Spatial Decomposition (R-PSD)

Step 3

When the CCP receives a task request from mobile clients, it uses the R-PSD to decide a geocast region that contains mobile servers in close proximity to the task and with high reputation level.

Step 4

Then, the CCP initiates a geocast communication process to all mobile servers within the geocast region geocast is used to direct contact mobile server. It is required to create some fake locations in the R-PSD. If allowed to contact mobile servers directly, the CCP can easily identify these fake points, and therefore breach privacy whenever it fails to establish a communication channel with some mobile servers. After receiving the task, a mobile server decides whether to accept the task or not.

Step 5

If the mobile server decides to accept the task, it replies with a message confirming its availability to the CCP. Otherwise, it does not reply and remains invisible to the CCP.



Fig.4.2 Privacybased model

4.3 MOBILE DEVICE BASED CLOUDLET MODEL

This model performs three functions: (i) Parameter monitoring (ii) Dynamic service time control (iii) Partially executed task state wrapping. This model monitors a number of cloudlet parameters including: user arrival rate, average number of users in the system and average time served. There are following main components:

i) Admission Control: This component admits the mobile device task to the cloudlet, admission control must monitor the number of tasks admitted into the system. The number of tasks entering into the system is recorded by service control and transmitted to the admission control.

ii)Task Execution:When the mobile user task is admitted to the cloudlet, then if the task is currently being served, it will be in execution state with task instructions being executed by one of the available CPUs.The task is submitted to service control component before re-entering the queue.

iii) Service Control (SC):

. First, it periodically manages the desired average service time Tds to ensure that the cloudlet performance is optimal and the mobile users get optimal response time for their submitted tasks.

iv) Task State Wrapper: If the task is not completely executed by the cloudlet, the mobile device needs to resume the task from the last process state in the cloudlet to be able to complete the task.

4.4 DYNAMIC DATA ALLOCATION SCHEME

In this scheme a novel hybrid on-chip SPM architecture consists of SRAM, MRAM, and Z-RAM is proposed. It has core which are coupled with on-chip SPM, which is composed of an SRAM, MRAM, and a Z-RAM. When core access a SPM Owned by itself it is called as local access while accessing other cores SPM is remote Access.



Fig. 4.4 system architecture

4.5. DYNAMIC RESOURCE ALLOCATION MODEL

In this model, a number of mobile devices are located in each other's vicinity. And this devices communicate with each other by D2D techniques. The working of this model is shown by task graph. Where task is denoted by nodes and it's processing by edges. When a node completes its task it is forwarded to succeeding node and in this way it execute task completely. In this case each node is act like MDs. In this way workload is offloaded.

5. ANALYSIS AND DISCUSSION

Task Allocation scheme shows the performance of TAS that is performed on different application profile Teach profile is selected independently and uniformly from the application pool with different task workloads and data communications [1]. The result shows that for every instance have considered, the performance is much better than the (1+E) bound and converges to the optimum as E decreases.Privacy-based framework shows how system overhead is reduced due to this scheme .As this scheme maintains reputation score [2], it shows that this algorithm have a large portion of mobile servers have high reputation scores. Mobile device based cloudlet model shows that 97% applications were able to complete their tasks faster under Mobile device based cloudlet model compared to cloudlet only execution.[3].It also shows that this model reduce cloudlet resource utilization.Dynamic data allocation algorithm shows that DDA algorithm can reduce the dynamic power consumption for a dual-core system and a quadcore system by 17.74% and 24.18%.Dynamic resource allocation

scheme shows that this approach results in highest overall task finish time. The task response time is reduced significantly [5].

6.PROPOSED METHODOLOGY

CLOUD MASKING TECHNIQUE

The main idea of the cloud masking technique is to present data differently to servers to preserve user's privacy. In this model all of the users are having same level of responsibilities instead to act as centralized or distributed servers. The proposed technique consists of following components:

1. Mobile client: At this level mobile client executes masking algorithm.

- 2. Mobile cloud server: Request is send to cloud server
- 3. Cloud providers: Cloud providers are selected based on nearest location.

The working of this technique is as follows:

Mobile clients executes masquerading algorithm and select leader. This leader then send query to cloud. Cloud identify users nearest cloud provider and transfer request to cloud server which is nearest to cloud provider. Cloud provider executes query and send it to cloud server. Server segregate answer with users Id and forward it to leader. Leader then send it to mobile client.



Fig.6.1 Cloud masking technique

Algorithm: STEP 1: Select Leader If found Send Request Else Again search for leader STEP 2: Send query to cloud STEP 3: select nearest cloud provider STEP 4: Send req to cloud server STEP 5: Executes query STEP 5: Executes query STEP 6: Check answer STEP7: Forward to leader STEP 8: Send back to client

In this way above algorithm improves the resource privacy using masking technique.

7. OUTCOME AND POSSIBLE RESULTS

The proposed cloud masking technique efficiently provides users privacy. It simply hide identity of user, So that its location is not known. In this technique, queries forwarded to next node is only known so that the initiator and final receivers are not known. As well as this technique helps in improving the system connectivity by selecting stable node as its next node.

8. CONCLUSION

This paper focused on different resource allocation monitoring scheme and introduced problems present in previous methodologies. To overcome this drawbacks this paper proposed a cloud masking technique that hide user's identity so that privacy is maintained.

9. FUTURE SCOPE

From observation, the scope is planned to be studied in future work, analysis will done on improving the privacy technique for resource allocation in mobile cloud computing.

REFERENCES

Journal papers

[1] Yi-Hsuan Kao, BhaskarKrishnamachari, Moo-Ryong Ra, Fan Bai"*Hermes: Latency Optimal Task Assignment for Resource-constrained Mobile Computing* "IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 16, NO. 11, NOVEMBER 2017

[2] Yanmin Gong, Chi Zhang, Yuguang Fang, Jinyuan Sun"*Protecting Location Privacy for Task Allocation in Ad Hoc Mobile Cloud Computing*" IEEE Transactions on Emerging Topics in Computing,2015

[3] MdWhaiduzzaman, AnjumNaveed, and Abdullah Gani "MobiCoRE: Mobile Device based Cloudlet Resource Enhancement for Optimal Task Response" IEEE TRANSACTIONS ON SERVICE COMPUTING, JUNE 2016

[4]MeikangQiu, Zhi Chen, Zhong Ming, Xiao Qin, and JianweiNiu" *Energy-Aware Data Allocation with Hybrid Memory for Mobile Cloud Systems*"IEEE SYSTEMS JOURNAL, VOL. 11, NO. 2, JUNE 2017

[5]Weiwei Chen, Chin-Tau Lea, Kenli Li"Dynamic Resource Allocation in Ad-Hoc Mobile Cloud Computing"IEEE 2017.