International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 03 | Mar-2016 www.irjet.net p-ISSN: 2395-0072

# Security concern in computation offloading Technique

**Priyanka Dnyaneshwar Patil**

*Department of Computer Engineering*

*Raisoni College of Engineering Jalgaon, Mahartashtra, India*

**Abstract:** *Nowadays, the increasing demand for mobile devices has led to increasing performance of mobile devices and due to this the battery life of mobile devices has been reduced. JADE is the software system that make use of computation offloading technique i.e it reduces some of the code from these mobile devices and reduces the burden of execution of code of these mobile devices which ultimately increases the battery life of mobile devices. But security problem arises when number of users make use of this computation offloading technique. So this paper presents the techniques i.e password technique and memorization technique for this purpose*

***Keywords-*** computation offload, password technique, memorization technique, mobile computing.

## 1.Introduction:

Nowadays, considering the increasing demand for mobile devices has led to increasing performance of mobile devices. The mobile devices consist of Android operating system, which consist of variety of facilities(i.e mailing, messaging, games, video calls, shopping etc). These mobile devices are created which powerful mobile processors, sensors and with large amount of energy.

The battery life has become biggest problem of these mobile devices. As these mobile devices consist of more powerful processors, sensors and more advanced features, they require more energy for operation which reduces the battery life of mobile devices.

The computation offloading is the technique that reduces the burden on these mobile devices. Computation offloading is the technique that deletes some of the code from these mobile devices and thus working of code is reduced

which ultimately saves the time for execution of the code and increases battery life of mobile devices.

The main problem arises due to security when extent of using this computation offloading technique is scaled up i.e when number of users are use this technique. When computation offloading is working on different users some data of many users may get mix with each other. To tackle security problem this paper present the following techniques

1. Password technique

2. Memorization Technique

The password technique work as follows:

- The password technique provides an algorithm in JADE that provides the password for mobile devices on which the JADE system is working.
- If the password for these mobile devices matches then only the users can use computation offloading technique.
- This password technique works serially i.e one by one password of the mobile devices are checked.

The memorization technique work as follows:

- The memorization technique provides separate memory for working of different users.
- This separate memory is volatile memory i.e after its operation the memory is exhausted.
- After is working the result is given back to the user.
- This technique works parallely i.e no. of users can use this technique at a time.

These both techniques contributes to the safe working of system.

## 2. Existing System :

In this section, we present the basic concepts of this computation offloading technique. There are various computation offloading techniques defined but the most effective, flexible, easiest one is JADE. JADE requires two mobile devices for its operation, one is client and another one is server. The client is the mobile device which offloads the code and server is the mobile device which executes the offloaded code(the code formed after offloading code). JADE is the software system which decides whether this offloaded code should be executed at client side or it should be executed at server side.

An application of mobile device is divided into small number of tasks. When this application performs the tasks JADE notices that some code of this application of client or server is useless and it should be offloaded then it take the decision that this offloaded code(i.e the code formed after offloading code)should be executed at client or server. JADE make use of EDP i.e Energy Delay Product formula for this purpose.

$$EDP = T*E=T^2*P$$

For task *i*, *T* is execution time of *i*

*E* is energy cost to execute *i*

*P* is average power consumption

to execute *i*

The client mobile device contains two buffers, buffer H (High computation) and buffer L ( Low computation). The task with high EDP value is task with high computation demand and is put into buffer H whereas the task with low EDP value is task with low computation demand and is put into buffer L. If any one of this buffer contains load of number of tasks then the work stealing strategy is used. Work stealing is job of stealing tasks from heavily loaded machine into lightly loaded machine. When The server also consist of two devices, device H (High Performance device) and device C ( Performance Constraint device ). If the buffer H contain more number of tasks then H device of server steals the tasks from buffer H and if buffer L contain more number of tasks then C device of the server steals the tasks from buffer L.

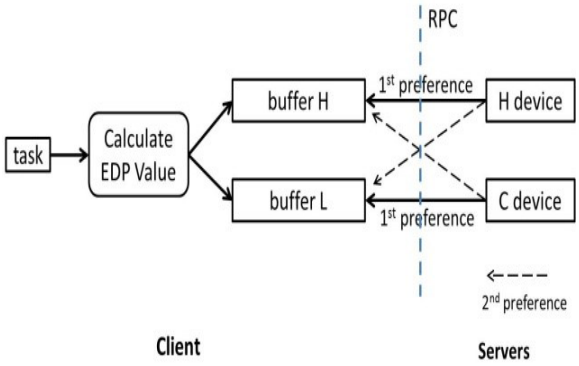


**Figure 1.1 :** Servers stealing tasks from buffers of the client

After this, the tasks when comes to server these tasks are again scheduled using HRRN (Highest Response Ratio Next) formula;

*Priority=(waiting time+estimated run time)/*

*(estimated run time)*

Where, waiting time is the time required to wait for jobs and estimated time is estimated time required to run the task.

In this way , the JADE reduces burden on the mobile devices and thus increase the battery life of the mobile devices.

## 3. Problems with existing System:

This section describes the problems with an existing system and techniques the problems can be overcome.

Although the computation offloading saves the battery life of mobile devices the security concern arises when the computation offloading technique is scaled up i.e number of users are using this technique. Sometimes the data of one task may go to another task, the results may overlap. In this case the security techniques must be given to the computation offloading technique. This section defines the two techniques for security.

1. Password Technique.
2. Memorization Technique

The sections 3.1 and 3.2 highlights the techniques for security. The section 3.1 describes the password technique which gives the password for task. The section 3.2 describes the memorization technique which allocates the

memory for task operation. The details of these techniques are given as follows:

### 3.1 Password Technique:

There are various techniques for security in computation offloading but the password technique offers more security and gives quick result in less time than any other technique. Password is the small word with characters, numbers, special characters etc. Password can be for single users or for group of user. The password for group of users is accessible to all users in group. This kind of password is used in company or organization where there is team work involved. The password for single user is used for user where only single user is involved. This kind of password is used when user is student of certain organization. The users in group can also have their individual password. The password can also be changed according to the situation.

The password technique creates the password for the task in application of the mobile device. The password is created for both the client mobile device and the server device. As explained earlier, an application of the mobile device everytime generates the task . The EDP value is then calculated for each of the generated. According to the EDP value, the task are given to the buffers in the mobile device. The servers then steals the task from client mobile device. When these task goes towards the server, the password is again generated for same task in server side. If both these password matches i.e password of task in client side and the password of the task in server then only the task is executed otherwise the task is not executed.

The stepwise working of the password technique in computation offloading is given as:

Step 1: The task is generated for application in mobile device.

Step 2: The password is generated for each task generated.

Step 3: The EDP value is calculated for each of the task generated.

Step 4: The task are assigned to the buffers according to the EDP value.

Step 5: Server steal the taskfrom client.

Step 6: Password is again generated for same task in server.

Step 7: If both the password matches then the task is executed otherwise not.

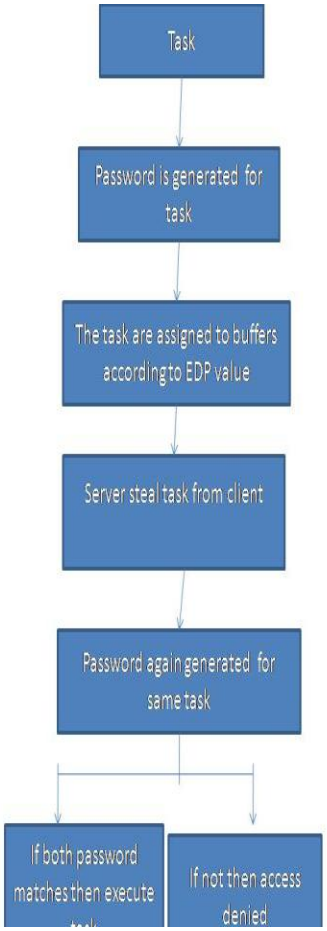


**Fig 1.2:** Working of password technique

In this way, the password technique for security in computation offloading works.

### 3.2 Memorization Technique:

The memory is the space allocated to the system to store the data of the system. The memory can be volatile or nonvolatile. The volatile is exhaustible kind of memory i.e when the power failure occurs the memory lost its data. The non volatile memory is the memory that saves the data even when power failure occurs. The same technique is used in computation offloading technique i.e it allocates the space for the tasks generated. As explained earlier, the tasks are everytime generated in an application of the

mobile device. The EDP value is then calculated for each of the task generated. After this, the tasks are assigned to the buffers according to the EDP value. Then the server steals the task from the clients and the separate memory is assigned to every task coming into the server. The task is executed in this memory separately. After its execution it return the result to an application and the memory is exhausted. The memory assigned to every task is volatile memory.

The stepwise working of memorization technique is given as follows:

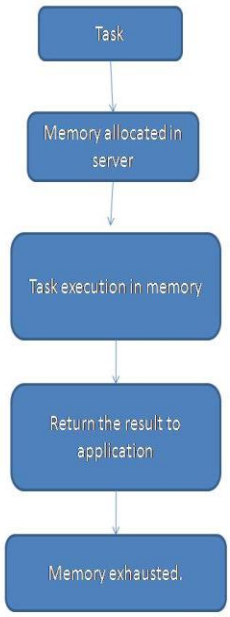


**Fig 1.3:** Working of memorization technique

Step 1: The task is generated for every application in mobile device.

Step 2: The EDP is calculated for each of the task generated in an application in mobile device.

Step 3: The task are assigned to buffers in client.

Step 4: Server steals the tasks from client.

Step 5: The memory is assigned to task in server automatically.

Step 6: The operation is done separately in memory i.e task is executed in memory.

Step 7: The result is returned to an application.

Step 8: The memory is exhausted.

In this way the memorization technique works in computation offloading and provides the security to the computation offloading.

### 3.2.1 Memory Profiling:

When the memory is assigned to the task in server the name or number is given to the memory. The database is created in system which keeps the track of memories assigned to the tasks. After its operation the memories are removed from database and is exhausted. The following components are used in memory profiling:

1. Memory Profiler
2. Communication manager
3. Optimizer
4. Compressor

*Memory Profiler:* As explained earlier, memory is assigned to the task in server, this assigning job of memories to the tasks is given by memory profiler. Moreover, the memory profiler also keeps track of the status of operation of task in memories, size of memories, giving name or numbers to the memories.

*Communication manager:* The communication manager is used for communication in system. It communicates for giving status of the memory, giving results after operation etc. All the operations in memory profiler, optimizer, compressor is done by communication manager.

*Optimizer:* The maximum size of memory to be assigned to the task. If an additional memory is required for task then optimizer works in that purpose.

*Compressor:* If an extra space in memory is left then compressor works in reducing the memory space.

All these components play important role in memory profiling. Memory profiling is most important factor in memorization as all working of it is dependant on profiling.

## 4. Conclusion:

In this paper, we presented techniques for security in JADE i.e password technique and memorization technique. Both the techniques can effectively provide security for

JADE which is computation offloading technique. Both these techniques are easy to understand and gives result in less time.

## References

[1] H. Qian and D. Andresen. "Jade: An Efficient Energy-aware Computation Offloading System with Heterogeneous Network Interface Bonding for Ad-hoc Networked Mobile Devices". In Proceedings of the 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/ Distributed Computing (SNPD), 2014.

[2] H. Qian and D. Andresen. "Extending Mobile Device's Battery Life by Offloading Computation to Cloud". In Proceedings of the 2nd ACM International Conference on Mobile Software Engineering and Systems (MOBILESoft), 2015.

[3] B. G. Chungs. "The techniques for security in computation offloading". In proceedings of 10th ACM International Conference on mobile ad-hoc networks, software engineering, computation offloading, 2014.

[4] E. Cuervo, A. Balasubramanian, D. Cho, A. Wolman, S. Saroiu, R. Chandra, and P. Bahl. "MAUI: Making smartphones last longer with code offload". In MobiSys, 2010.

[5] B.G.Chungs. "Security provision in mobile ad hoc networks". In proceedings of 14th AICS Conference on mobile security. 2015.

[6] Q. Chen, H. Qian et al. "BAVC: Classifying Benign Atomicity Violations via Machine Learning". In Advanced Materials Research, Vols 765-767, pp. 1576-1580, Sep, 2013.

[7] L. Peng, Y. Yang et al. "Highly Accurate Video Object Identification Utilizing Hint Information". In proceedings of the International Conference on Computing, Networking and Communications (ICNC), 2014.

[8] S. Zhang, X. Zhang and X. Ou. "After We Knew It: Empirical Study and Modeling of Cost-effectiveness of Exploiting Prevalent Known Vulnerabilities Across IaaS Cloud". In proceedings of the 9th ACM Symposium on Information, Computer and Communications Security (ASIACCS), 2014.

[9] B. Satval, "Mobile security". In proceedings of 7th ACM International Conference on mobile ad-hoc networks, mobile communication ,security.