# Toward Advance Resource Reservation in Mobile Grid Configurations Based on User-Centric Authentication

**Matheus A. Viera[1], Cristiano C. Rocha[1], Michael A. Bauer[2], Miriam Capretz[3], M. A. R. Dantas[1]**

[1]Dept. de Informática e Estatística – Universidade Federal de Santa Catarina (UFSC)
Caixa Postal 88040-900 – Florianopólis – SC – Brazil

[2]Dept. of Computer Science – University of Western Ontario, Canada

[3]Dept. of Electrical & Computer Engineering – University of Western Ontario, Canada

{matviera,crocha}@inf.ufsc.br, bauer@csd.uwo.ca, mcapretz@eng.uwo.ca, mario@inf.ufsc.br

***Abstract.*** *There has been growing interest in the use of mobile devices for providing access to the various applications, services and resources within grid computing environments. As is the case for most access to grid resources, the use of mobile devices requires user authentication. Given the limited amount of power available for mobile devices, the applications on these devices, including the authentication services used to access grid resources, must be designed to conserve power. In this paper, we present an authentication architecture utilizing a "lightweight" user-centric authentication approach. Specifically, we aim to provide mobile users with access to advance resource reservation within grid environments, and, consequently, our approach incorporates this objective. The approach, however, applies to user authentication with any grid resource or service. In attempting to overcome the limitations of mobile devices, such as limited battery power, mobile users can utilize grid environments in a transparent and secure way.*

## 1. Introduction

A Grid computing is characterized by making a variety of distributed resources, including services, devices and applications, available to a wide range of users [Foster 2002]. Various organizations, both real and virtual, can make different types of resources available under dynamically changing availability constraints and with varying policies for access and use of these resources [Foster et al. 2001]. Subsequently, the resources belonging to these organizations can be accessed and combined by different users to achieve their computational goals.

As a result of their nature, grids provide a variety of services that users can incorporate for achieving their computational tasks. Specifically, users can access resources, applications and services, submit jobs for execution either via queues or by advance reservation, create combination processes in workflows, and verify the status of jobs or systems. However, access to most grid environments requires some form of security and user authentication. In this context, authentication involves the process of establishing the digital identity of a user or object to use the network, applications or resources. Once authenticated, a user can access the resources based on the permissions that they have been granted, which are established through the authorization process.

In recent years, there has been a movement towards integrating grid computing environments with mobile computing environments [Rossetto et al. 2007; Chu and Humphrey 2004; Gomes et al. 2007]. Consequently, mobile devices within this context are considered as grid interfaces and as grid resources. Despite the fact that the computing power of mobile devices has improved significantly in recent years, the current processing power and storage capacity found in these devices are still not enough to solve complex problems. Therefore, the present study considers the use of mobile devices as interfaces to access the resources and services of a grid from anywhere, at anytime. Our approach aims to enable users to utilize mobile devices for access to advance reservation services with the objective of submitting individual tasks and workflows. As is the case with other access to grid services, the use of mobile devices also requires a user authentication mechanism, which is a device that allows users to adopt defined or permitted roles for access to the services and resources.

As studies in area of mobility suggest, a change in the approach of performing user authentication via mobile applications, namely, from a process-oriented paradigm to a user-centered one, must be accomplished [Saha and Mukherjee 2003]. Specifically, the authentication system should recognize the user rather than the equipment that the user possesses. Moreover, because mobile devices have limited power, authentication schemes that are computationally intensive or that require substantial communication are unsuitable. This change to a user-centered approach, coupled with the limited power resources of mobile devices, imposes new requirements on the security and authentication systems for supporting the use of mobile devices within grid environments.

The current work presents an architecture that provides a “lightweight” user-centric authentication mechanism for the use of mobile devices within grid environments. In particular, its purpose is to provide the user with the full range of mobile service offered by these environments. Accordingly, our approach to authentication is in the context of providing the mobile user with access to resource reservation services.

The paper is organized as a series of sections; the motivation for the development of our approach is presented in Section 2. The proposed architecture is introduced in Section 3, and Section 4 presents the experimental results. Finally, the paper presents our conclusions and future research work in Section 5.

## 2. Motivation

The research in [Rossetto et al. 2007], a previous work of our group, proposes a framework for submitting and monitoring grid computing tasks through mobile devices. In that study, there is a mechanism for managing disconnections that result from a drop in battery power or from interference in the wireless network. However, this framework poses a disadvantage in the case where a user accesses different devices during the execution of an application. In this situation, each device must perform the entire authentication process, thus reducing the battery charge and the system productivity.

Furthermore, this work does not examine access to an advance resource reservation facility in the grid environment and uses a traditional authentication where a username and password are requested in each interaction.

Advance resource reservation in the grid computing environment has been the focus of recent research (e.g., [Takefusa et al. 2008], [Siddiqui et al. 2005] and [Roblitz and Reinefeld 2005]). By reserving resources, a client has guaranteed access to a specific resource in the grid for a designated time period. Accordingly, [Takefusa et al. 2008] and [Siddiqui et al. 2005] present mechanisms for resource reservation using the concept of co-allocation [Foster et al. 1999], which can be defined as the simultaneous use of grid resources across multiclusters. The approach described in [Takefusa et al. 2008] provides resource reservation for a single resource or for a set of resources by using co-allocation. In addition, the work suggests the use of a ticket for subsequent interaction with the reservation. In [Siddiqui et al. 2005], the authors present an approach that uses the Web Service Resource Framework (WSRF) [Globus Alliance 2010] to perform resource reservation, along with the introduction of a two-phase commit protocol. Their objective is to use a non-blocking mechanism that avoids disconnection problems and can facilitate the recovery of failed processes. While [Takefusa et al. 2008] suggests the use of co-allocation, [Roblitz and Reinefeld 2005] introduces the idea of virtual resources without co-allocation. The elimination of this mechanism allows the generic integration of different types of resources and reservations with the use of temporal and spatial relationships between components.

On the other hand, because of the movement from a process-based paradigm to the user-centric paradigm, some studies present requirements that must be considered for user-centric security systems. Therefore, in order to fulfill these requirements, it is necessary to analyze context-related information, such as the user's location, the time in which the interactions occur and the context-based detection of anomalous transactions [Mashima and Ahamad 2008]. According to Johnson [Johnson 2009], in highly dynamic environments as mobile grid environments, context-aware security mechanisms are necessary because the change of context is used by these mechanisms to allow the adjustment based on the current situation. Therefore, these mechanisms are able to effectively circumvent limitations of traditional security systems that are designed for static environments and are not suitable for the mobile computing paradigm. Several works present complex solutions for user authentication based on the environmental context [Choi and Yi 2008; Babu and Venkataram 2009]. Most of these studies achieve their objectives by using several sensors in these environments. However, these proposals restrict user mobility because they are only effective within the area covered by the sensor network. For instance, [Choi and Yi 2008], presents an architecture that aims to authenticate users based on the context captured by various sensors and devices present in the "smart homes" environments. Additionally, [Babu and Venkataram 2009] proposes an authentication scheme regarding the analysis of the user behavior. Even tough this study presents a module concerned with the power consumption of mobile devices regarding the required level of authentication, it is not able to consider the device switching that can be performed in mobile environments.

Nevertheless, these studies neglect the possibility of advance resource reservation and the possibility of monitoring an application through mobile devices. In addition, there are several research efforts to improve mobile environments, but none of these studies present user-centric authentication methods or consider alternatives for reducing battery consumption. Since frequent problems, such as the disconnection of mobile devices in wireless networks could lead to application faults and high energy consumption, it would be necessary to run the authentication process over again, leading to more power usage.

## 3. Proposed Architecture

In this section, we propose a user-centered architecture that enables advance resource reservation in grid environments. Our approach is partially based on the research presented in [Rossetto et al. 2007], where the authors propose a framework for the submission, monitoring and coordination of workflows executed in grid computing environments. All of the interaction with the grid is performed through mobile devices that are used as grid interfaces. In particular, this work suggests the possibility of adapting the execution flow to guarantee the consistency of an application in case of a disconnection occurs. This execution flow will be performed in a personalized way in the case that the mobile device is disconnected from the network regarding the dependences among the tasks. Specifically, these features are performed by **Workflow Manager, Agent** and **Mobile GUI.**

The **Workflow Manager** module is responsible to manage the requests processes from mobile devices in a transparent way to the users. In particular, it provides an automated way of submitting jobs to the grid and it collects information about the execution of these jobs without user interaction. Thus, this mechanism contributes to the reduction of battery power consumption in mobile devices. Also, the architecture provides a mechanism for fault tolerance, especially in the case where a voluntary or involuntary disconnection of mobile devices occurs. **The Agent** module is responsible for verifying when the disconnection occurs; if the device is connected, it uses a specific time interval. Additionally, this module also manages the faults by detecting the failure and adapting the application execution flow to the environment. When a disconnection occurs, **The Agent** can adapt to the situation by continuing the execution, waiting for device establish a connection or aborting. These options are defined by the user, and the actions are performed according to the existence of dependencies from the user. Hence, through this module, the consistency of the application is guaranteed.

All grid computing interactions occur through a **Mobile GUI** interface. This interface is responsible for allowing workflow submission and permitting the visualization of final and partial results of the application in an optimized way, since only the parts of the resulting files that are considered relevant for the user are loaded in the device interface. Also, the interface contains the ability for users to monitor the application execution, so that the status of each task can be traced. In addition, users can monitor the application execution in a customized manner based on the type of mobile device and its particular screen size. Finally, the **Mobile GUI** is responsible for sending the username and password to **Workflow Manager** for authenticating the user on the grid environment. Consequently, the user has to authenticate every interaction with the grid through their mobile device.

In addition to **Workflow Manager, Agent** and **Mobile GUI**, as proposed by

Rossetto et al. [Rossetto et al. 2007], the modules of **User-centric Authentication** and **Resource Reservation** were added in the present approach for enabling a more secure and more efficient interaction in mobile grid environments. The new modules attempt to take advantage of the  mobility offered by mobile devices while utilizing the resources from grid environments more safely and effectively. In addition to these goals, our approach attempts to improve the battery consumption of mobile devices.

Figure 1 illustrates the research architecture of [Rossetto et al. 2007] with the addition of the new modules, User-centric Authentication and Resource Reservation, which are added to the proposed framework.

### 3.1. User-Centric Authentication

The mobile computing paradigm suggests that the procedures are focused on the user regardless of the device that he/she is using. Therefore, the objective of the user-centric authentication module consists of providing the user with the advantages offered by mobile devices, such as Personal Digital Assistants (PDAs) and smartphones, in grid environments. These advantages include the possibility of anytime and anywhere access to the grid. Moreover, grid access in a safe, transparent and automatic manner is also part of the current work.

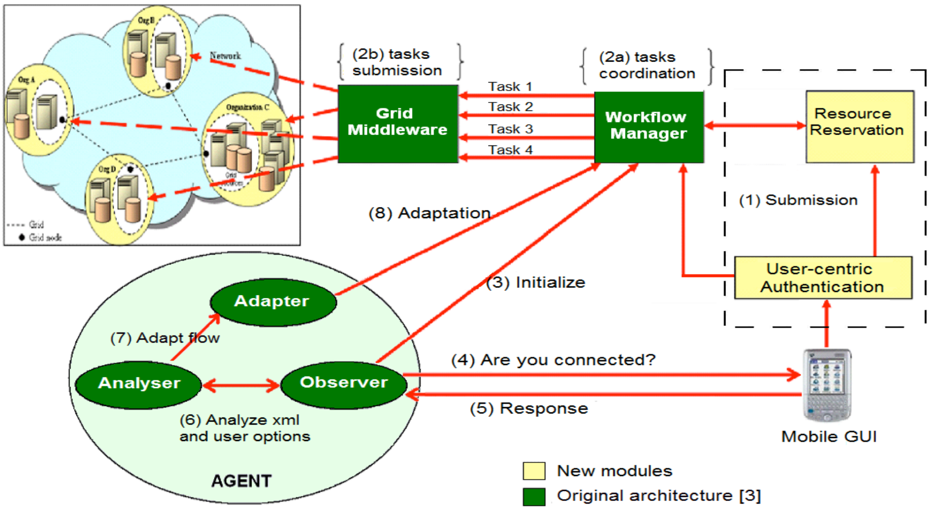
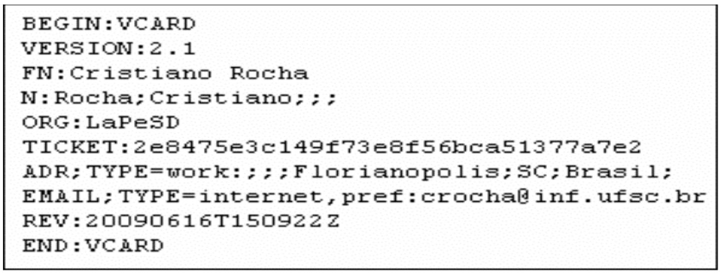


**Figure 1. Proposed architecture**

Through device independence, which is referred to as user-centric computing throughout this paper, the user can switch from an equipment to another without requiring a new authentication process. Thus, the potential problem of insufficient battery power can be avoided by device replacement. Moreover, the user's interaction with an application communicating with the grid environment is not interrupted, nor is it necessary to restart the authentication process. The authentication module is responsible for the interception of all service requests, which are workflow submissions or advance resource reservations requested by an individual using a mobile device. This authentication approach obtains transparency by using a widely disseminated standard among mobile devices: the vCard standard [Dawson and Howes 1998], which aims at the automation of personal information sharing frequently found in a regular identification card. In this standard, the data is presented by using pre-defined meta-information that is responsible for receiving data in an organized manner and then facilitating the utilization of the data. The standard has been maintained by the Internet Mail Consortium (IMC) since 1996; the vCard standard is compatible with several existing platforms and is mainly concentrated on mobile devices, such as cell phones and PDAs.

Furthermore, the vCard standard permits the extension of meta-information in order to store other necessary data. Thus, it permits greater flexibility in the manipulation of user information and in the adequacy of each required application. The inserted information does not affect the original standard because it is ignored by the interpreter. Subsequently, the unity guarantee is maintained among various applications that involve the exchange of the same electronic identification card. Furthermore, this standard provides security for the stored information, because it offers support for digital signatures.

Therefore, the authentication system uses the vCard standard to store system-specific information. This information, such as environmental access credentials, or tickets, is represented by strings that are created by the system and that have a predetermined duration, which depends on the permissions granted to the user. For a user that has permission to reserve resources, the ticket could expire at the time of the reservation. Thus, while the lifetime of the user ticket is limited, the user can utilize other devices that have the properly formatted vCard in the system. In other words, the device has the vCard extended, so that the user does not need to reinsert his access data in the system. Figure 2 shows an example of credential represented by the vCard standard.



```
BEGIN:VCARD
VERSION:2.1
FN:Cristiano Rocha
N:Rocha;Cristiano;;;
ORG:LaPeSD
TICKET:2e8475e3c149f73e8f56bca51377a7e2
ADR;TYPE=work:;;;Florianopolis;SC;Brasil;
EMAIL;TYPE=internet,pref:crocha@inf.ufsc.br
REV:20090616T150922Z
END:VCARD
```

**Figure 2. Example of an extended electronic identification card represented in the vCard format**

The user-centric authentication module and its interactions with the other system modules are shown in Figure 3. The authentication process is used to prove the digital identity of the user. When the user requests a service, the system accesses the vCard in the device. (I) The **Credential Manager** selects the specific credentials of the application that are contained in the vCard and verifies if the user is on the list of active users; in other words, it verifies if the ticket is still valid. If the ticket has expired, (II) the **Credential Manager** queries the **Device Manager** to verify if the user switched to a different device. If a switch has occurred, (III) the **Location Manager** performs the functions illustrated in the activity diagram in Figure 4. Otherwise, it determines if there is an association between the user and the device used in the request. If such an association exists, the **Ticket Manager**, which controls the lifecycle of the tickets, creates a new ticket. Consequently the **Credential Manager** updates the vCard with the new ticket, and subsequently, the updated vCard is stored in the **Credential**

**Repository**, and it is also sent to the device. Otherwise, if the user cannot be associated with the device, the system requests the login and the password of the user. (IV) If the ticket is still valid, the **Permission Manager** is queried in order to verify that the user has the permission for the requested operation. If the user has the appropriate permission, (V) the request is sent to execute the requested operation. This operation is one of the available services, along with resource reservation, reservation cancelation and the submission and monitoring of downloaded application results, the latter of which is also provided in [Rossetto et al. 2007]. Finally, the operation response requested by the user is returned to him/her (VI).

Moreover, since one of the main goals of the user-centric authentication module is the securityof the user's information in the environment, all messages sent between themobile devices, **Mobile GUI**, and the **Credential Manager** are encrypted. Therefore,this procedure tries to prevent malicious users from acquiring unauthorized access togrid services.

In recent years, mobile devices are able to perfom geometric models used to determine object location with geographic coordinates. These models are commonly used by location models based on the GPS (Global Positioning System). Thus, due to the advantages offered by applications that are able to facilitate location-related queries and manage accurate information regarding the location of objects, the latest generation mobile devices is being equipped with GPS to provide support for these applications. Also, it is possible to configure the accuracy of the location in order to safe battery of mobile devices. Therefore, the integration of these two popular technologies, vCard and GPS, which is still under development in the authentication system, is responsible to improve the security offered to users in the environmnent .The next section describes the functionalities of the authentication system regarding the user's location.

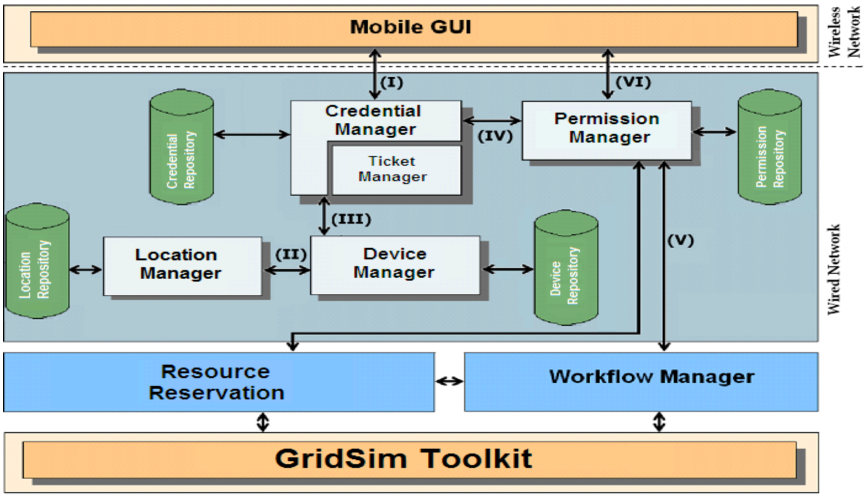


**Figure 3. Authentication module architecture and its interaction with the others modules**

### 3.1.1. Spatio-Temporal Analytical Model

In order to provide more reliability to the mobile grid environment as well as to minimize and detect fraudulent activities, the authentication system considers the capacity of the mobile devices to capture information regarding the spatio-temporal context of the environment where they are inserted. Thus, the **Location Manager** can classify the performed activity (event) regarding the geographic location and the time frame of occurrence of this event simultaneously. In order to formally define an event, we assume that an event is an interaction (activity) of the user with the application or environment in a certain location and at a particular time frame. Then, an event is described as:

$$E_i = < operation, time, location >$$

Therefore, the observed events in the execution of activities form a database (**Location Repository**) for the process of detecting information clusters, which translates to the behavior of users. These clusters can be classified into three broad categories: purely spatial, purely temporal or spatio-temporal. In purely spatial clusters, the occurrence is higher in some regions than it is in others, and purely temporal clusters feature the occurrence of events as being greater in a certain period than it is in others. Finally, spatio-temporal clusters occur when events are temporarily higher in certain regions than they are others. Among the models used to predict events in a spatio-temporal context, we propose the use of spatio-temporal permutation, which allows the incorporation of covariate information found in other contexts within the pervasive space. The Poisson model, which is applied to purely temporal contexts, and the Bernoulli model, which is preferably applied to spatial contexts, were both rejected because they do not consider both the location of the user and the time frame during an occurrence of an event.

According to Kulldorff [Kulldorff 2010], the spatio-temporal permutation model is based on three characteristics: *i)* detecting data clusters in space and time simultaneously; *ii)* working with only events or cases; and *iii)* applying the probabilistic model in a null hypothesis to conclude that the events follow a hypergeometric distribution.

Assuming the count of events ***e***, in the timeline set in ***t***, located in a region ***z***, with circular features according GPS coordinates, is defined as $\boldsymbol{e_{zt}}$. The total number of observed events ***E*** and the total number of conditioned events $\boldsymbol{M_{zt}}$ are expressed by the following formulas:

$$E = \sum_z \sum_t e_{zt} \qquad\qquad M_{zt} = \frac{1}{E}\left(\sum_z E_{zt}\right)\left(\sum_t E_{zt}\right)$$

The prediction of an event encompasses the following assumption: the conditional probability of an event $\boldsymbol{P(E_a)}$ in the region ***z*** was observed at the time $\boldsymbol{t_1}$ and $\boldsymbol{t_2}$, defined in a particular cylinder ***a***, which reflects a possible cluster; therefore $\boldsymbol{E_a}$ has an average $\boldsymbol{M_a}$ and follows the hypergeometric distribution determined by the following function:

$$M_a = \sum_{(z,t)\in A} M_{zt} \qquad\qquad P(E_a) = \frac{\begin{pmatrix} \sum\limits_{t\in(t_1 \vee t_2)} \sum\limits_{z\in A} E_{zt} \\ E_a \end{pmatrix} \begin{pmatrix} E - \sum\limits_{t\in(t_1 \vee t_2)} \sum\limits_{z\in A} E_{zt} \\ \sum\limits_{t\in(t_1 \vee t_2)} \sum\limits_{z\in A} E_{zt} - E_a \end{pmatrix}}{\begin{pmatrix} E \\ \sum\limits_{t\in(t_1 \vee t_2)} \sum\limits_{z\in A} E_{zt} \end{pmatrix}}$$

In order to determine the regions of the clusters, it will be used the *SaTScan* tool developed by Kulldorff [Kulldorff 2010] and the statistical significance will be validated by using the hypothesis test of Monte Carlo.

The conditional probability of the user ***P(E$_a$)*** allows the system to estimate what kind of activity the user was performing and what one he is currently performing when he moves from a mobile device to another one. Thus, there are four cases that can occur: *i)* the same activity in the same spatio-temporal context – it is defined as a normal execution; *ii)* same activity in different spatio-temporal contexts – it is defined as a suspicious execution, but some properties must be considered such as the velocity of mobility in order to apply the appropriate authentication policies; *iii)* different activities in the same spatio-temporal context – it is defined as a suspicious execution; and *iv)* different activities in different spatio-temporal context – it is defined as an abnormal execution. Therefore, depending on the categorization of the user, the authentication system defines which action will be taken regarding the following factors: the performed request, the malicious user, the mobile device and the potential fraud victim. The activity diagram shown in Figure 4 illustrates how the system operates when it detects device switching.

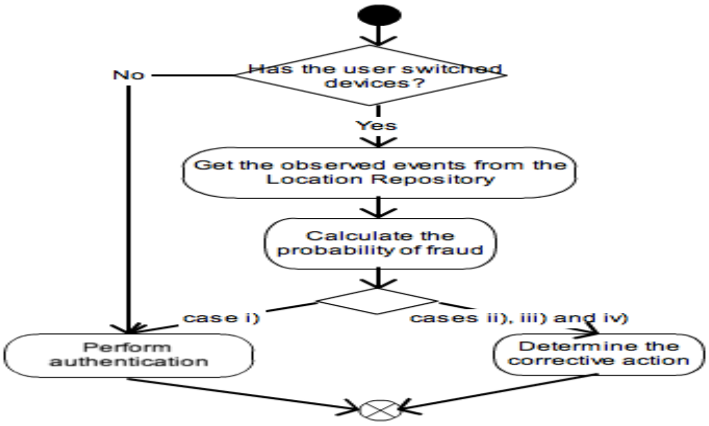

Has the user switched devices?
No
Yes
Get the observed events from the Location Repository
Calculate the probability of fraud
case i)
cases ii), iii) and iv)
Perform authentication
Determine the corrective action

**Figure 4. Fraud detection activity diagram**

### 3.2. Resource Reservation

As previously discussed, the possibility of resource reservation allows mobile users to plan their future use of the grid. The resource reservation module, which is still under development, is responsible for ensuring that these reservations are maintained for future workflow submission on the grid. In addition, it enables the monitoring of reserved resources as well as recording any cancelled reservations. Figure 5 illustrates the design of the module and its functionality is described in the subsequent paragraphs.

First, after intercepting the request and authenticating the user, the authentication service transfers the ticket access information and the resources requiring reservation to (I) the **Reservation Service**. At the same time, the authentication module transfers the start time and end time of the reservation to the **Reservation Service**, which uses (II) the **Grid Information Service (GIS)** to verify the availability and status of the requested resources. If there are available resources, (III) the **Co-allocation Service** will select the best option based on the information from the **GIS**, and it will allocate the resources accordingly. At this point, the user ticket is associated with the reservation, which enables future interactions between the user and the system, allowing the user to verify the status of reservations, cancel a reservation or monitor the workflows. Subsequently, information pertaining to the allocated resources and the user ticket are stored in (IV) a **Data Base** (DB), hence enabling a checkpoint mechanism. This method is necessary in case a user wishes to access a previous workflow result or interact with the grid environment to submit or cancel workflows.

The ticket created by the authentication module might specify a duration time based on the time of the reservation. When a ticket is no longer valid, the resources reserved by the user are automatically released. When the user submits a workflow to the environment, the Reservation Service searches the information in the Database to verify the user ticket. Once the ticket is verified, the workflow is sent to the **Workflow Manager** (V).

Through the reservation module, users can plan the future use of resources based on their mobile requirements. Since the reservation is performed and monitored through their mobile device, the user does not need to worry about which device will make submissions and monitor workflows. Rather, they need to ensure that the resources have been previously allocated.

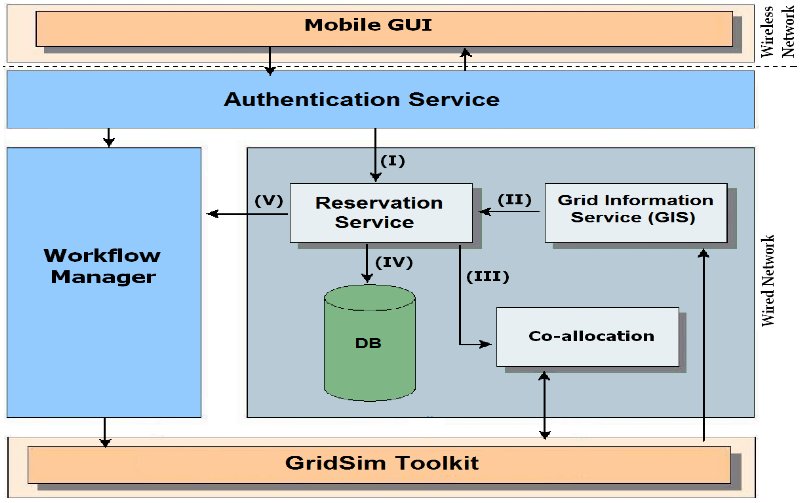


**Figure 5. Resource reservation architecture**

The development of the resource reservation module was enabled by GridSim [Sulitio and Buyya 2004]. The toolkit supports modeling and simulation of heterogeneous grid resources, users and application models. This toolkit will assist with the implementing the Reservation Service component, modeling heterogeneous computational resources of variable performance, and testing the policy of advance resource reservation.

## 4. Experimental Results

Our experiments were performed on the basis of the environmental configuration proposed in [Rossetto et al. 2007] and focus on the battery usage without concern about potential security threats. Therefore, the Java programming language was used for implementing the user-centric authentication service and integrating it with the other modules. In addition, the module present in the Mobile GUI, which is responsible for handling the user's vCard and intercepting service requests, was implemented using the J2ME (Java 2 Micro Edition) Wireless Toolkit. In addition, the simulator GridSim was used as the grid environment.

The experimental environment consisted of a server containing the authentication service, which was integrated with the other modules presented in [Rossetto et al. 2007]. Also, the mobile devices used in our experiments were two Palm Tungsten C devices, each with a 400MHz processor, 64 MB RAM, built-in Wi-Fi (802.11b), and a Palm OS 5.2.1 operating system. As the integration of GPS with authentication system is still under development, for the current experiments we used a device without GPS.

Since the maintenance of battery life is one of the most critical and challenging problems found in mobile devices, such as PDAs and cell phones [Mohapatra et al. 2005; Rong and Pedram 2003], new methods and techniques are required to reduce the dissipation of energy in such devices. Accordingly, we analyzed the efficiency of the proposed user-centric authentication mechanism based on the power consumption of mobile devices.

This analysis was performed by identifying a pre-defined sequence of ten service requests. Specifically, this analysis compared the execution of a sequence using the user-centric authentication approach and the traditional authentication approach. The traditional authentication approach refers to the device-centric authentication method used in [Rossetto et al. 2007], where a username and password are requested when the user moves from one mobile device to another. The device-centric authentication was chosen for analysis because it is one the most common authentication mechanisms in mobile grid environments, as indicated in the research. In order to evaluate the efficiency of the mechanism proposed in this paper, we simulated a user changing mobile devices. Therefore, the pre-defined requests were interspersed between the two devices by performing the pre-defined sequence in a mobile device, then running it in the other one.

Figure 6 presents empirical results using the battery consumption of the mobile devices as the metric for the performance of the proposed approach, which compared user-centric authentication to the traditional authentication. This evaluation was performed using the BatteryGraph software [Witteman 2010], which had been installed on the mobile devices. It provides the mean battery level, expressed in milivolts (mV), before and after the completion of each of the two applications.

Figure 6 indicates that the user-centric authentication approach demonstrates a consistent increase in power consumption based on the number of requests. In comparison, the traditional authentication approach causes a greater increase in the energy consumption of the battery. Thus, the proposed approach represents a significant reduction in the power consumption of the battery as compared to the traditional authentication mechanism.

The second experiment attempted to analyze the efficiency percentage of the proposed mechanism. Specifically, it consisted of running the same sequence of pre-defined requests several times until the battery was totally depleted. First, this procedure was performed using the traditional authentication approach and switching the mobile devices between the sets of requests. Subsequently, the same experiment was performed by executing the application with the user-centric authentication mechanism. As in the case of the traditional approach, this execution also used the process of interspersing the sets of requests between the two mobile devices. In addition, in order to acquire an accurate assessment, both experiments were performed three times.

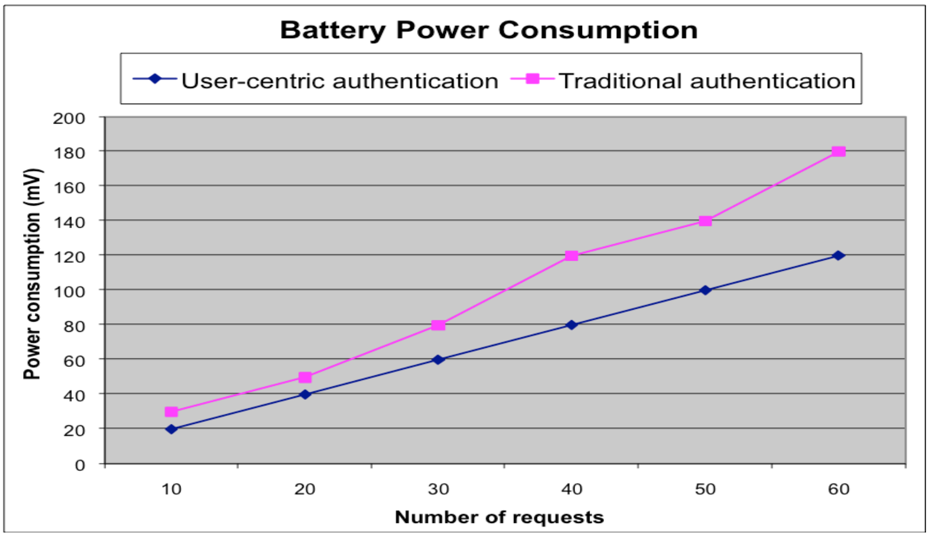


**Figure 6. Battery power consumption for two authentication approaches**

Figure 7 presents the results obtained by using the two authentication approaches. The BatteryGraph was utilized for obtaining the percentage of the devices' charge level. Moreover, it also verifies the percentage of battery used during a time interval selected by the user.

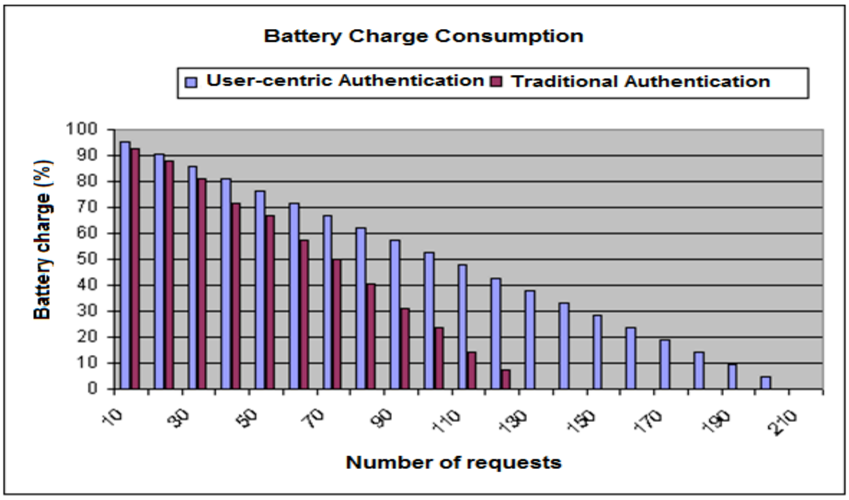


**Figure 7. Comparison of battery charge for two authentication approaches**

As shown in Figure 7, the mechanism proposed in this work for user-centric authentication enables a greater autonomy of energy in comparison to the traditional authentication mechanism. For instance, the traditional authentication mechanism resulted in total battery exhaustion after 130 requests, while the proposed approach for user-centric authentication did not completely drain the battery until after 200 requests. Therefore, the user-centric authentication approach results in a noticeable increase of approximately 53% in the battery life.

## 5. Conclusions and Future Work

This paper proposed an approach for enabling safe advance resource reservation in mobile grid environments by adopting the user-centric authentication approach. The proposal addressed the shortcomings in [Rossetto et al. 2007], which were mainly due to the inefficiency of various components in the environment. This work aimed to create a safe and transparent system for users to submit tasks and reserve resources in mobile grid environments. Specifically, its primary objectives consisted of making the user's interaction with the environment more flexible and reducing the battery consumption of mobile devices, both of which were successfully achieved. In addition, the proposal also aimed to provide to the user with more efficient mobility resources in such environments.

Although it is recognized that there is a need for experiments focused on other relevant requirements in mobile grid environments such as interactivity of the user, behaviour of the authentication service when there are disconnections and interferences in the wireless network and the ability of the system in detecting frauds. This study has demonstrated that the proposed approach for user-centric authentication illustrates the improved performance of battery life in comparison to the traditional authentication approach for mobile grid environments. This improvement indicates that a significantly greater number of operation requests can be performed by the user that operates multiple mobile devices during his interaction with the environment. Therefore, the approach proposed in this paper provides a more productive environment for the user.

As an extension of the current research, we intend to perform further simulations using other mobile device models in order to perform experiments regarding the user's location and the impact on the experience of the user. Moreover, we will consider other important metrics in mobile grid environments, such as the occurrence of disconnections and interferences in the wireless network, user interactivity, and the ability of the system in detecting frauds. In addition, we intend to evaluate the latency of the user-centric authentication approach, particularly, the way in which it affects the resource reservation environments. Although this implementation only represents one type of improvement, we believe that the design implications presented in this study are applicable to other scenarios.

## References

Babu, S. and Venkataram, P. (2009) "A dynamic authentication scheme for mobile transactions", International Journal of Network Security, vol. 8, pp. 59-74.

Choi, H. and Yi, Y. (2008) "An user-centric privacy authorization model based on role and session in the context-aware home", Proceedings of the 8th IEEE International Conference on Computer and Information Technology Workshops, pp. 254–259.

Chu, D. and Humphrey, M. (2004) "Mobile OGSI .NET: Grid computing on mobile devices", Proceedings of the 5th IEEE/ACM International Workshop on Grid Computing, pp. 182–191.

Dawson F. and Howes, T. (1998) "RFC2426: vCard MIME directory profile", RFC Editor, USA.

Foster, I. (2002) "What is the grid? A three point checklist", GridToday, vol. 1, no. 6.

Foster, I., Kesselman, C. and Tuecke, S. (2001) "The anatomy of the grid: Enabling scalable virtual organizations", International Journal of High Performance Computing Applications, vol. 15, no. 3, pp. 200-222.

Foster, I., Kesselman, C., Lee, C., Lindell, B., Nahrstedt, K. and Roy, A. (1999) "A distributed resource management architecture that supports advance reservations and co-allocation", 7th International Workshop on Quality of Service, pp. 27–36.

Globus Alliance (2010) "The WS-Resource Framework", http://www.globus.org/wsrf/

Gomes, A., Ziviani, A., Lima, L. and Endler, M. (2007) "DICHOTOMY: A resource discovery and scheduling protocol for multihop ad hoc mobile grids", Proceedings of the 7th IEEE International Symposium on Cluster Computing and the Grid, pp. 719–724.

Johnson, G. (2009) "Towards shrink-wrapped security: A taxonomy of security-relevant context", Proceedings of the 7th IEEE International Conference on Pervasive Computing and Communications, pp. 1-2.

Kulldorff, M. (2010) "SaTScan v7.0: Software for the spatial and space-time scan statistics", http://www.satscan.org/

Mashima, D. and Ahamad, M. (2008) "Towards an user-centric identity-usage monitoring system", Proceedings of the 3rd International Conference on Internet Monitoring and Protection, pp. 47–52.

Mohapatra, S., Cornea, R., Oh, H., Lee, K., Kim, M., Dutt, N., Gupta, R., Nicolau, A., Shukla, S. and Venkatasubramanian, N. (2005) "A cross-layer approach for power-performance optimization in distributed mobile systems", Proceedings of the 19th IEEE International Parallel and Distributed Processing Symposium, vol. 11, pp. 8.

Roblitz, T. and Reinefeld, A. (2005) "Co-reservation with the concept of virtual resources", 5th IEEE International Symposium on Cluster Computing and the Grid, vol. 1, pp. 398–406.

Rong, P. and Pedram, M. (2003) "Extending the lifetime of a network of battery-powered mobile devices by remote processing: a markovian decision-based approach", Proceedings of the 40th Conference on Design Automation, pp. 906–911. ACM New York, NY, USA.

Rossetto, A., Borges, V., Silva, A. and M. Dantas (2007) "SuMMIT – A framework for coordinating applications execution in mobile grid environments", Proceedings of the 8th IEEE/ACM International Conference on Grid Computing, pp. 129–136.

Saha, D. and Mukherjee, A. (2003) "Pervasive computing: a paradigm for the 21st century", IEEE Computer, vol. 36 no. 3, pp. 25–31.

Siddiqui, M., Villazon, A., Prodan, R. and Fahringer, T. (2005) "Advanced reservation and co-allocation of grid resources: A step towards an invisible grid", Proceedings of 9th IEEE International Multitopic Conference, pp. 1–6.

Sulistio, A. and Buyya, R. (2004) "A grid simulation infrastructure supporting advance reservation", Proceedings of the 16th International Conference on Parallel and Distributed Computing and Systems, pp. 1-7, MIT, Cambridge, USA.

Takefusa, A., Nakada, H., Kudoh, T., Tanaka, Y. and Sekiguchi, S. (2008) "GridARS: An advance reservation-based grid co-allocation framework for distributed computing and network resources", LNCS, 4942, pp. 152-168.

Witteman, J. (2010) "BatteryGraph", http://palm.jeroenwitteman.com