

**EFFICIENT QUEUE AND GSI SECURITY
MANAGEMENT FRAMEWORK FOR MOBILE
DESKTOP GRID**

By


MUHAMMAD IMRAN SARWAR

**Thesis submitted in partial fulfillment of the
requirements for the degree of
Masters of Science**

June 2008

DECLARATION

This dissertation is the result of my own work except where specifically indicated in the text. I am aware that the degree awarded will be forfeited in the event of plagiarism.

Signature: .....
01/07/08

Date: 1st July 2008

Name: (Muhammad Imran Sarwar)

ACKNOWLEDGEMENTS

Firstly, I wanted to thank Almighty Allah, the most merciful, the most beneficial for giving me the opportunity to do my masters and my research dissertation from University Sains Malaysia.

I realize I wouldn't have reached my destination without the help of several people. I am deeply indebted to my supervisor, Dr. Chan Huah Yong who helped me sail through rough waters and unfamiliar territories to reach this destination. He fostered my research skills and presentation abilities, but most of all, he taught me to always keep a positive attitude.

I am extremely grateful to Professor Dr. Rosni Abdullah the Dean, School of Computer Sciences for her encouragement and very important advices. My endeavors would not have been successful without her.

My sincere gratitude goes to all Grid Computing Group members, especially Mike, Aloysius, Homam, Adel, Ali, Muzzammil and George, for providing various kinds of help when I was most needed. I have learnt many valuable things from them.

I am extremely grateful to my lovely parents Dr. Muhammad Sarwar and Rifat Bano, my sisters Ainee and Ayesha. They have prepared me for this long-lasting trek. The successful completion of my work is the fruit of their sacrifices, their devotion and their determination.

I thank all of my friends especially Hamid, Mohsin, Qasim, Zhen Ling, Mohanad and especially my best buddy Ahmed Al-Madi, for being the friends everybody could wish for. We shared many wonderful moments together and we were there for each other through good and bad times.

Last but not least, my warmest and sincerest thanks to my respected elder brother Usman and his wife Haniya. They are always there when I need them the most. This thesis is the outcome of your scrutinizing my thesis with your critical and careful review. I pray to all for the best in their life.

Table of Contents

DECLARATION	ii
ACKNOWLEDGEMENTS	iii
LIST OF TABLES	viii
LIST OF FIGURES	ix
ABSTRACT	xiii
CHAPTER 1 - INTRODUCTION	1
1.1. Introduction.....	1
1.2. Wireless Grid Computing	1
1.3. Background.....	3
1.4. Problem Statement	4
1.5. Objectives	5
1.6. Scope of the thesis.....	6
1.7. Main Contribution	6
1.8. Outline of the thesis.....	7
CHAPTER 2 - LITERATURE REVIEW	8
2.1. Introduction.....	8
2.2. Proxy based Mobile Grid Architecture.....	9
2.2.1. Overview	9
2.2.2. Review of Proxy-based Architecture	10
2.2.3. Data Cache Management Framework in Mobile Device	14
2.2.4. Security Architecture in mobile grid computing	16
2.2.5. Network Infrastructure of Mobile Grid Computing.....	21
2.2.3. Summary of Proxy-based Architecture.....	22
2.3. Comparison of Proxy-based Architectures	23
2.4. Summary.....	23
CHAPTER 3 - RESEARCH METHODOLOGY	25
3.1. Overview.....	25
3.2. Proposed Methodology Architecture.....	26
3.2.1. Methodology Overview	26

3.2.2. Methodology Design Attributes	27
3.3. JRMS Framework Architecture	28
3.3.1. Overview	28
3.3.2. Components of JRMS Framework	29
3.3.4. Interaction components in Mobile Desktop Client	37
3.3.5. Interaction of Mobile Desktop Client with the Proxy Node.....	38
3.3.6. Communication Process of Mobile Desktop Client.....	40
3.4. PRMS Framework Architecture.....	41
3.4.1. Overview	41
3.4.2. PRMS Framework Architecture	41
3.4.3. Components of PRMS Framework.....	42
3.4.4. Grid Security Infrastructure (GSI).....	43
3.4.5. Summary	44
3.5. Lightweight Encryption Algorithm	44
3.5.1. Blowfish Overview	45
3.5.2. Blowfish Cryptography Architecture.....	45
3.5.3. Blowfish Cryptography Algorithm.....	46
3.6. Justification.....	48
3.6.1. Lightweight Framework.....	48
3.6.2. Less Cache Size Limit	48
3.6.3. Lightweight Cryptography Algorithm	48
3.6.4. Platform Independent.....	49
3.7. Summary.....	49
CHAPTER 4 - DESIGN AND IMPLEMENTATION	50
4.1. Introduction.....	50
4.2. Software Resource Specifications	50
4.2.1. Programming Language.....	50
4.2.2. Programming IDE.....	51
4.2.3. Operating System	51
4.3. Application Prototype Implementation.....	51
4.3.1. JRMS Queue Management Framework.....	51
4.3.2. PRMS Result Management Framework.....	59

4.4. Summary..... 65

CHAPTER 5 - EVALUATION AND RESULTS 66

5.1. Introduction..... 66

5.2. Hardware Resources 66

5.2.1. Mobile Clients 66

5.2.2. Grid Proxy Server..... 67

5.3. Quantitative Research Evaluation 68

5.3.1. Test Setup..... 68

5.3.2. Experiments and their Evaluations 69

5.4. Qualitative Research Evaluation 77

5.6. Summary..... 79

CHAPTER 6 - CONCLUSION AND FUTURE WORK 80

6.1. Summary..... 80

6.2. Summary of Objectives & Contributions 81

6.3. Comparison with Related Work..... 82

6.4. Future Research Work..... 83

References: 84

LIST OF TABLES

	Page
Table 2.1. Comparison of Proxy-based Architecture Frameworks	23
Table 4.1. Important Classes of JRMS Framework	52
Table 4.2. Important Classes of PRMS Framework	60
Table 5.1. Hardware specifications of mobile devices	67
Table 5.2. Grid Proxy Server Hardware Specification	68
Table 5.3. JRMS Queue Statistical Data Analysis of Mobile Devices	71
Table 5.4. Qualitative Research Evaluation	78
Table 6.1. Comparison of JRMS and MAGI Framework	82

LIST OF FIGURES

	Page
Figure 1.1. Basic Architecture of the mobile Grid Computing (Kalim, U., et al, 2005)	3
Figure 2.1. Broadview of the proxy based clustered architecture (Phan, T., et al, 2002)	11
Figure 2.2. Proxy Architecture for Mobile Client (Millard, D., et al, 2005)	12
Figure 2.3. Mobile Grid Proxy Architecture (Guan, T., et al, 2005)	13
Figure 2.4. Deployment model & architecture of MAGI (Kalim, U., et al, 2005)	14
Figure 3.1. Mobile Proxy Grid Infrastructure	26
Figure 3.2. Architecture of JRMS Framework	28
Figure 3.3. JM saving Job Request	30
Figure 3.4. JM retrieving Job Request	31
Figure 3.5. Job Message Save in JRQC	32
Figure 3.6. Job Retrieve from JRQC	33
Figure 3.7. Work flow of NM	35
Figure 3.8. Working flow of the Cryptography Manager	36
Figure 3.9. Sequence diagram of components in Mobile Desktop Client	37
Figure 3.10. Working flow of the mobile proxy grid	39
Figure 3.11. Process sequence of inter-communication process of mobile client	40
Figure 3.12. PRMS Framework Architecture	41
Figure 3.13. Feistel Structure of Blowfish (Ferguson, N., and Schneier,	46

	B., (1994))	
Figure 3.14.	Round function of Blowfish (Ferguson, N., and Schneier, B., (1994))	46
Figure 3.15.	Blowfish encryption algorithm (Ferguson, N., and Schneier, B., (1994))	46
Figure 3.16.	Blowfish decryption algorithm (Ferguson, N., and Schneier, B., (1994))	47
Figure 3.17.	Function (F) (Schneier, B., 1993)	47
Figure 4.1.	Class diagram of the Mobile Desktop Application Framework	53
Figure 4.2.	View of Job Request Form GUI in the mobile client	56
Figure 4.3.	GUI screen on 3 different mobile devices	56
Figure 4.4.	Class diagram of Grid Proxy Server	61
Figure 5.1.	JRMS framework Test setup of experiment	69
Figure 5.2.	Comparison of the JRMS on tablet-pc, hand-top and notebook	72
Figure 5.3.	Job submission comparison using Blowfish & GSI PKI Cryptography	74
Figure 5.4.	File encryption using Blowfish & DES Cryptography in tablet-pc	75
Figure 5.5.	File encryption using Blowfish & DES Cryptography in hand-top	75
Figure 5.6.	File encryption using Blowfish & DES Cryptography in notebook	76

SIRI DAN SEKURITI GSI KERANGKA PENGURUSAN YANG EFISIEN BAGI GRID KOMPUTER MEJA MOBIL

ABSTRAK

Kemajuan dan perkembangan yang amat besar dalam teknologi barangan pegang-tangan telah membuatkan pihak pengkaji berfikir akan cara untuk menggunakan kuasa alat-alat mobil dalam bidang arkitek yang begitu luas berhubungan dengan Penggunaan Komputer Bergrid. Peralatan mobil mempunyai sumber komputer dan kuasa operasi yang terhad, isu-isu lain yang terbatas dalam persumberan komputer adalah seperti jaringan terselindung, ketidaksinambungan jaringan yang kerap berlaku, penggunaan tenaga bateri, sekuriti dan kualiti servis dan lain-lain. Salah satu kajian pendekatan untuk membangkitkan isu ini ialah bidang arkitek proksi grid yang mobil dimana, alat-alat mobil berkomunikasi dengan alat servis proksi grid yang menghantarkan permintaan ke grid komputer bagi pihak alat mobil itu, dengan itu ia memperolehi kebanyakan daripada kegunaan grid komputer.

Kajian ini mencadangkan siri mesej kerangka pengurusan bersiri Sistem pengurusan permintaan kerja (JRMS) untuk menguruskan mesej bersiri pada media simpanan tempatan semasa ketidaksinambungan jaringan dan menyambung semula selepas itu. Kerangka JRMS adalah paling tegap untuk menghadapi kegagalan jaringan kawasan liputan dan juga kelemahan kuasa bateri. Sumbangan kedua kajian ini ialah kerangka sokongan Pengurusan Keputusan untuk Proksi Grid (PRMS) untuk proksi grid yang menyimpan meklumat klien, jika mobil klien terganggu kesinambungannya tanpa memperolehi maklumat. Kajian ini menggunakan sistem mudah autentik berdasarkan

kata-laluan bersama dengan algoritma kriptograph ringan Blowfish untuk sekuriti penyampaian data yang dikehendaki oleh alat mobil ke alat servis proksi grid dan sebaliknya. Kami mengesahkan kajian kami ini berdasarkan penilaian kajian yang dibuat secara kuantitatif dan kualitatif. Keputusan eksperimen ini membuktikan bahawa kerangka JRMS adalah efektif serta efisien bagi alat-alat mobil.

EFFICIENT QUEUE AND GSI SECURITY MANAGEMENT FRAMEWORK FOR MOBILE DESKTOP GRID

ABSTRACT

Tremendous advancement and growth in the hand-held technology make the researchers think to utilize the power of mobile devices into the vast architecture of the Grid Computing hence lead to the new paradigm of mobile grid computing. Mobile devices are resource limited and have many issues such as computational resources limitations, network latency, frequent network disconnection, battery power consumption, security etc. To address these issues, researchers proposed mobile proxy grid architecture in which mobile devices communicated with grid proxy server which sends the request to the computational grid on behalf of the mobile device hence gets the most of the functionality of the grid computing.

This research proposes message queue management framework **Job Request Management System (JRMS)** for managing the messages on the local storage media while on disconnection and sends the request later. JRMS is robust against network coverage and battery power failure. Second contribution is **Proxy Result Management System (PRMS)** for grid proxy that save client result, if mobile client gets disconnected without receiving the result. This research uses simple password-based authentication system along with lightweight Blowfish cryptography algorithm for secure data request transmission from the mobile device to the grid proxy server and vice versa. We justify our work on the basis of quantitative and qualitative research evaluation. The experimental results prove that JRMS framework is effective as well as efficient for mobile device.

CHAPTER 1 - INTRODUCTION

1.1. Overview

The term 'Grid' in computer science is specifically referred to a concept that is designed for sharing the resources that are in the form of files, data, different software (operating systems, programming language, applications etc.) and heterogeneous hardware (cluster of pc, mobile, tablet-PC, PDA, laptop etc) in a distributed systems in order to get maximum computational performance for solving complex and ambiguous computational problems in an effective and efficient manner.

The hardware resources in grid are autonomous and managed in a distributed manner. They are aggregated in a large global network to form a computational grid, by which huge workload can be compiled and completed with maximum performance gain and throughput. (Foster, I., 2002) provides three criteria to recognize Grid. "A Grid coordinate resources not under centralize control uses standard, open, general-purpose protocols and interfaces and delivers nontrivial qualities of service."

1.2. Wireless Grid Computing

The wireless grid computing advances and grows the capabilities of traditional grid computing paradigm by including wide range of mobile and embedded devices which interacts with each other to share resources in order to solve computational intensive problem. In the same way, mobile grid computing is also considered as a new

paradigm in a wireless grid computing which gives advantage in terms of mobility, portability and wireless communication (Kalim, U., et al, 2005).

According to (McKnight, L. et al, 2004), “Wireless Grids is a new type of resource sharing network that connects sensors, mobile phones, and other edge devices with each other and with the wired grid. Ad hoc distributed resource sharing allows these devices to offer new resources and location of these grid computing”.

Everyday there is a new advancement in wireless devices technology in terms of computational processing power and other capabilities and functionalities. They become new extension of grid computing paradigm, providing those new resources as well as challenges (Phan, T. et al, 2002) and (McKnight, L. et al, 2004). Wireless grid shares number of characteristics with the traditional grid computing which are their distributed nature of architecture, same protocols and communication standards and high demand of security and quality of service QoS (Agarwal, A. et al, 2004).

(McKnight, L. et al, 2004) groups wireless grid applications into three categories that sometimes overlaps based on their unique attributes:

1. Applications which collect and aggregate data.
2. Applications which take advantage of the locations in which they can exist or can move to;
3. Applications which take advantage of the cooperation amongst a mesh of mobile devices.

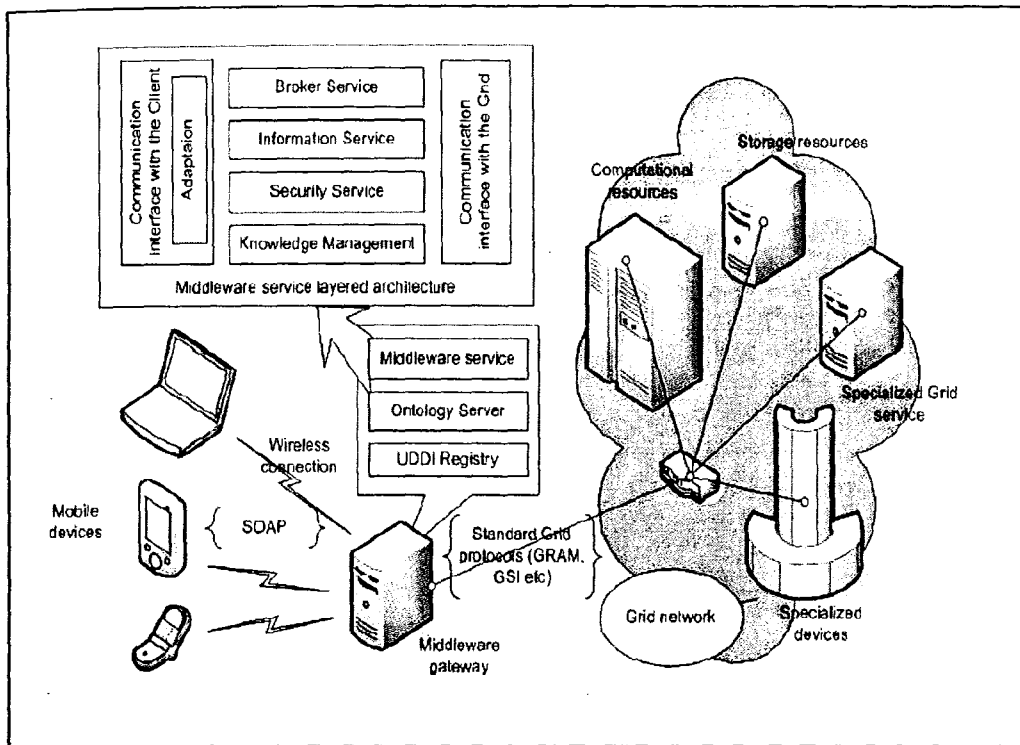


Figure 1.1: Basic Architecture of the mobile Grid Computing (Kalim, U., et al, 2005)

1.3. Background

There is a tremendous advancement and growth in the hand-held technology, computing and communication capabilities, rapid proliferation of the mobile devices, and decreasing device costs. By analyzing this, researchers around the world figure it out that why not utilize the power of these mobile devices into the vast architecture of Grid computing when they are in the idle mode and taking advantage of their mobility. These mobile devices are becoming as powerful as our desktop PCs, thereby attracted many researchers to think about it. Of course, the mobile grid computing inherited same properties from the general grid computing like distributed in nature, standard for communication & protocols, security and quality of service issues.

Apart from the bright sides of the mobile grid computing, it is noteworthy to consider some unpredictable problems which are inherited due to their hardware limitation i.e., less computation power, network latency, often communication disconnection, power consumption etc.

1.4. Problem Statement

Firstly, traditional mobile devices in the mobile grid computing are thin client or browser based. Mobile devices are used for showing information or results in their browser. As they are not robust against network coverage failure, so when mobile device want to compute or send a message and there is not network coverage available, the message will be lost. Secondly, mobile grid computing is lacking behind in terms of security due to number of key factors which includes limited resources, computational power etc. The security components used in the traditional grid cannot be ported to the mobile grid because of the computational and resource limitation of the mobile device and lack of proper network infrastructure. This research will highlight the following set of issues:

- Lack of effective, lightweight and efficient data request management framework for major type of mobile devices which preserve the data when mobile device gets powered off or disconnected from the network.
- Lack of compact middleware framework for grid proxy server which provides the recovery mechanism for the job result received from the computational grid when mobile gets disconnected without receiving the result.

- Lack of efficient, lightweight and secure authentication mechanism for mobile devices in the mobile proxy grid architecture

1.5. Objectives

The goal of this research is to investigate, propose and enhance an existing framework which provides a lightweight message queue management system and authentication mechanism that is suitable for resource limited mobile devices in order to provide data integrity over wireless network. The key objectives of this thesis are as follows:

- To propose Job Request Management System (JRMS) framework compatible with major type of mobile devices (i.e., hand-top device, tablet-pc, notebook etc) that will manage job request when network is disconnected or battery powered off.
- To propose Proxy Request Management System (PRMS) middleware framework architecture for grid proxy server which will preserve the results of the job requests in the local disk as a backup.
- To incorporate lightweight password-based authentication system along with layer of lightweight cryptography layer between mobile device and the proxy grid server.

1.6. Scope of the thesis

The scope of this thesis is limited to research, use and enhance lightweight framework suitable for mobile desktop grid in mobile proxy grid architecture. The Job Request Management System (JRMS) is lightweight framework architecture which is suitable for the resource limited mobile devices. Each component doesn't require much computational and memory power. This research work also concentrate on the security component which consist of authentication mechanism and secure channel between the mobile devices and the grid proxy server achieved by cryptography. We will review the existing cryptography algorithms and select one which is efficient, lightweight and well suitable for this research work. We argue and justify our work by set of experiments and evaluations based on quantitative and qualitative research evaluation.

1.7. Main Contribution

The main contributions for this research are:

1. Enhanced Message Queue Management Framework JRMS for the major high-end mobile devices
2. Enhanced Result Management Framework PRMS for the grid proxy server
3. To use lightweight cryptography algorithm along with password-based mechanism for secure communication in mobile desktop grid architecture

1.8. Outline of the thesis

This research thesis is organized in six chapters which are briefly discussed below:

Chapter 2 contains a review of literature relevant to present topic and study. This review begins with the general introduction of the mobile grid computing and researcher's contributions in the proxy-based architecture of the mobile grid computing. The literature further continues with the review of cache and queue management framework in the mobile devices, security and network infrastructure in mobile grid computing architecture.

Chapter 3 explains the research methodology of JRMS framework architecture. The chapter starts with the methodology overview and attributes, then further explains the JRMS client side and server side architecture. For the secure layer between the mobile devices and the grid proxy server, Blowfish cryptography algorithm is also explained. The chapter ends with the justification of the research methodology.

Chapter 4 gives in-depth information of the design and the implementation of this research work. Important set of mobile client and grid proxy server class is been mentioned along with their respective class diagrams.

In **Chapter 5**, we conduct set of scenarios, to evaluate JRMS framework in terms of quantitative and qualitative research aspects. We further present the evaluated results in graph and tabular forms. Finally in **Chapter 6**, we concluded this thesis with research work summary, revisiting the objectives, contributions and present the future work.

CHAPTER 2 - LITERATURE REVIEW

2.1. Overview

Mobile grid computing is interesting research area for the researchers due to its rapid growth in technology and cost effectiveness. The number of organizations and researchers around the world are discovering to take advantage of mobile devices and finding new ways to utilize the power of mobile devices in grid computing. With the help of mobile ad hoc network (MANET), these devices connect to the internet, following a peer-to-peer networking architecture. As a result, they are taking advantage of the resources of the wired grid and also giving them their own resources to the wired grids (McKnight, L. et al, 2004). When there are large numbers of wireless devices making the above infrastructure get available, then the potential of the ad hoc network becomes very vast dramatically (Phan, T. et al, 2002).

The main advantages of the mobile grid computing is its ability to interact with the mobile-to-mobile and mobile-to-desktop collaboration for sharing resources, innovative user experience, convenience and novel application experience. The grid-based mobile environment will allow mobile devices to interact effectively and efficiently by off-loading resource demanding to more powerful devices and computers (Millard, E. at al, 2005).

Although mobile device facilitates the user by giving the advantage in terms of primary resources and computing platform but they also have serious limitations in terms of computational power, storage area and above all the security prospective (Millard, E. et al, 2005). In the same way, these problems and limitations are very

unique due to their mobility as compared to the traditional wired network. The number of devices available in a wireless grid can be unpredictable because at any point they can leave and some other devices can join the network. The device can be disconnected due to battery power loss, by movement out of the communication coverage or probably by turning the device off by the user (Ahuja and Myers, 2006). Additional complexities are related to the authentication of devices and the users when they enter the grid environment (Ahuja and Mayers, 2006).

In this section of the thesis, detail literature review of the mobile proxy grid along with important components based on the proxy grid architecture, data saving and security mechanism is elaborated.

2.2. Proxy based Mobile Grid Architecture

2.2.1. Overview

The mobile devices are now increasingly popular throughout the globe. Researchers around the world are figuring out the way to port functionality of traditional grid to the mobile devices hence making the mobile grid computing architecture. There are many issues in porting the grid functionality to the resource limited mobile devices especially in terms of computational resources and memory etc. One of the ways to get the same attributes of grid computing in the mobile computing is through the use of proxy as a middleware between the mobile devices and the computational grid.

2.2.2. Review of Proxy-based Architecture

In this section, some related literature work is presented with regards to mobile proxy grid architecture:

2.2.2(a). LEECH

Barely Adequate Systems Leveraging Internet NEtworking (BASELINE) acronym was established by (Phan, T., et al, 2002) for mobile devices and were among the first one to proposed a framework based on proxy-based clustered architecture. They suggested using heterogeneous mobile devices connected through unreliable wireless network. They presented a challenge of harvesting the increasingly popular wireless mobile devices such PDAs and laptops that can be emerged in the traditional grid computing architecture. In their proposed work LEECH, they proposed a proxy-based cluster design in which multiple baseline mobile units (called minions) are integrated with the computational grid. They created N-baseline units that are connected with the proxy node called “interlocutor” which can either be baseline or non-baseline unit. The interlocutor interacts with the computational grid on behalf of the minions. Generally, the accessed difficulties involved in the integrating of the mobile devices with the computational grid computing. They argued that proxy can address many issue concerning about the integration of both paradigms and suggested that their model is indeed an economical model.

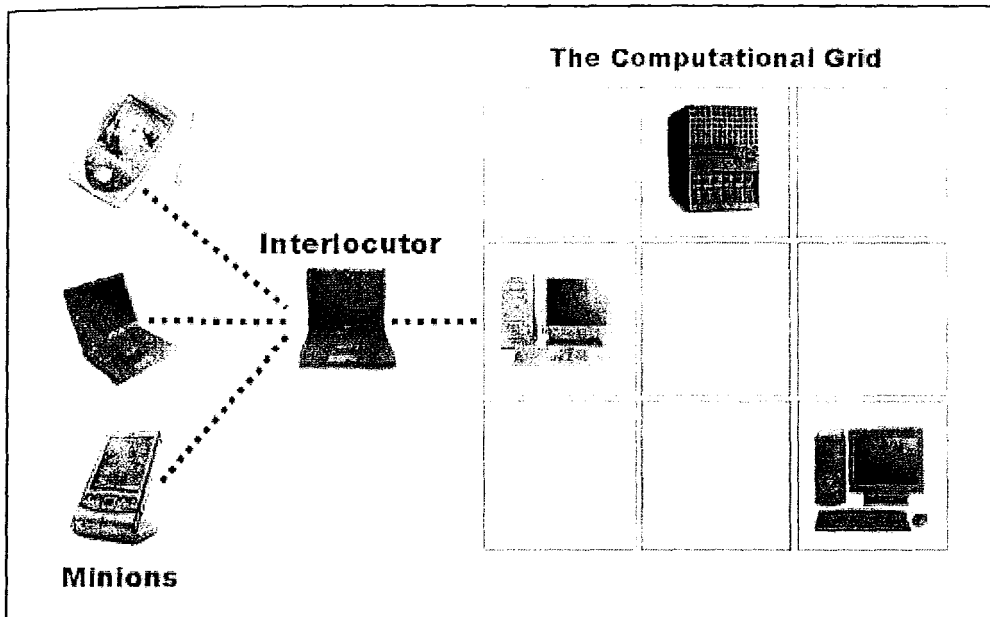


Figure 2.1: Broadview of the proxy based clustered architecture (Phan, T., et al, 2002)

2.2.2(b). FINESSE

(Millard, D., et al, 2005) implemented the mobile Grid client for finesse (Finance Education in a Scalable Software Environment), an existing web-based e-learning system. The scope of their work was only based on the exploring the feasibility of the mobile devices as a Grid Platform. They explore different language technology like .NET to invoke remote grid services from mobile devices, java to have common and cross platform feature and lastly by proxy architecture to invoke grid service via web server.

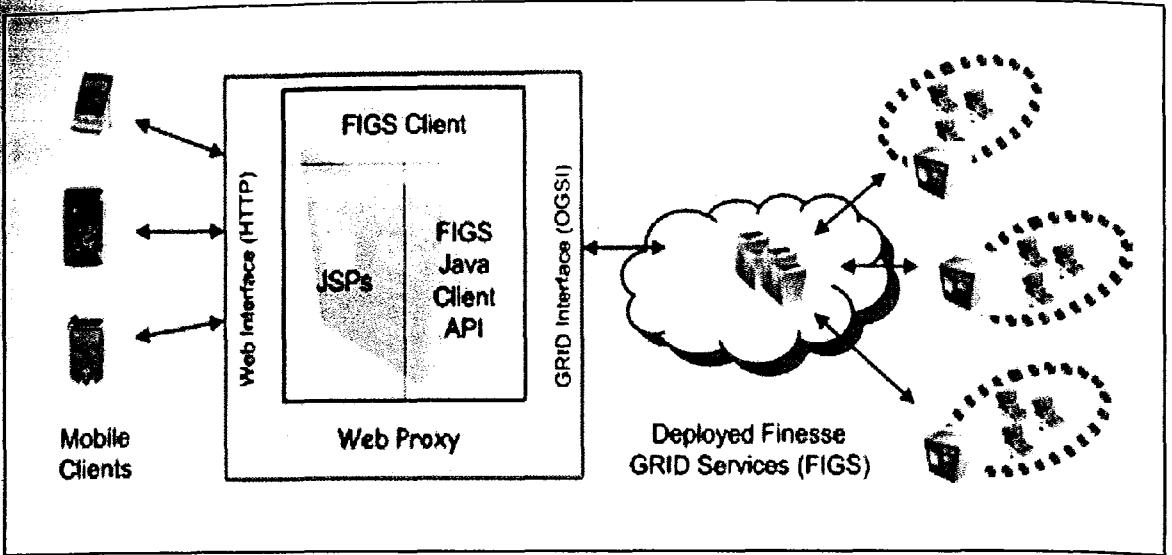


Figure 2.2: Proxy Architecture for Mobile Client (Millard, D., et al, 2005)

2.2.2(c). Proxy Architecture based on Grid Services

(Guan, T., et al, 2005) presented a system architecture that allows the local mobile devices to interact with the computational grid through a proxy middleware using grid services. In their architecture, there are three important modules each have their own functionality. Execution Module is invoked by device proxy module and is responsible for sending small script file to the proxy node, Personal Information Module stores the user information and the Cache Module stores the information module in order to transmit same information multiple times. Virtual machine technology has been implemented in the proxy node in order to achieve complete isolation, flexibility, resource control etc.

The mobile device transfers the request to the proxy command, which will enable proxy to download the application execution code, then its installation and finally

execution of the application. As its beyond the scope of the proxy to execute the application generate the result, so the proxy send the application to the grid, which then computes and send back the result.

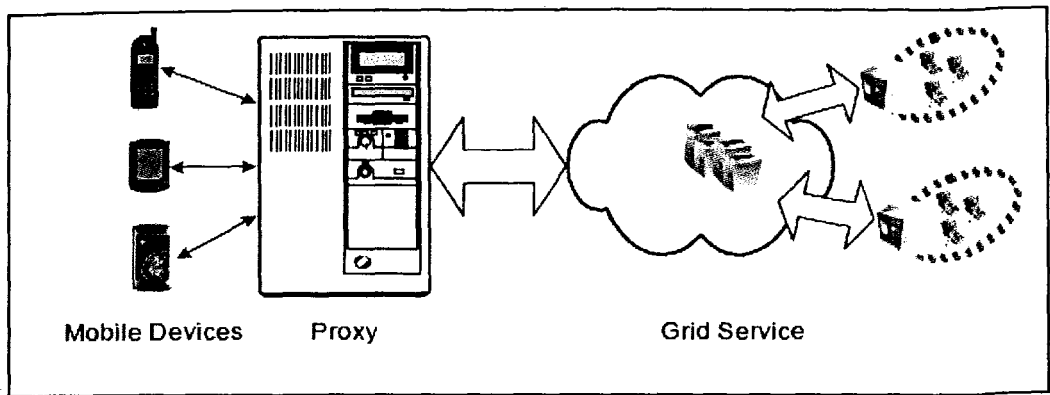


Figure 2.3: Mobile Grid Proxy Architecture (Guan, T., et al, 2005)

2.2.2(d). MAGI

(Kalim, U., et al, 2005) presented a proxy middleware architecture for the mobile grid computing named as MAGI (Mobile Access to Grid Infrastructure). MAGI addresses the important issues like job delegation to the grid services, message management for the offline mode (either disconnection or battery power off), secure communication using combination of Elliptic Curve and AES Cryptography between mobile device and the proxy node. Last important feature of their MAGI framework was the ability to interact with homogeneous mobile devices and present the result according to their device specification and limitations. They demonstrate their work by giving resource intensive task to the mobile devices.

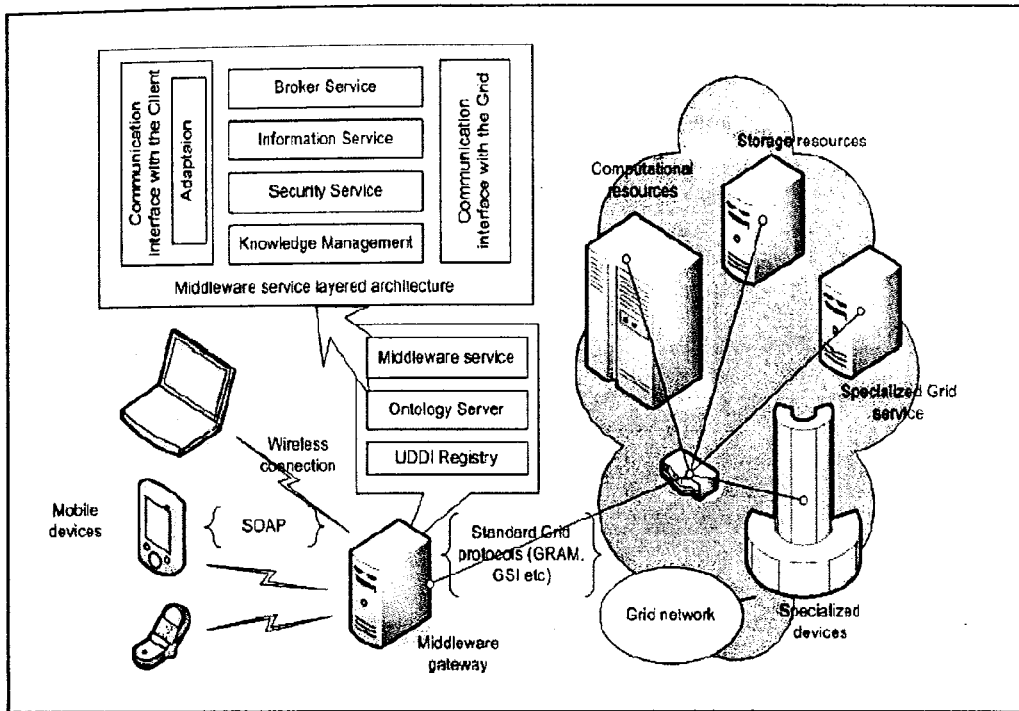


Figure 2.4: Deployment model & architecture of MAGI (Kalim, U., et al, 2005)

In this research work, enhancement will be made in the mobile proxy grid architecture on 2 important components which are explained below

1. Data Cache Management Framework in Mobile Grid Computing
2. Security Architecture of Mobile Grid Computing

2.2.3. Data Cache Management Framework in Mobile Device

2.2.3(a). Overview

Data cache management in mobile device is an important factor in order to improve the performance of the mobile devices, prevent the data from being lost after the network disconnection occurs. But maintaining the mobile cache is hard job itself

especially when we consider the issues which occur due to the wireless network and limited mobile computational resource power. The major issues are limited storage space for variable data size, frequent disconnection, data update procedure and infrequent battery power loss etc.

2.2.3(b). Review of Cache Management Framework

(Xu, J., et al, 2004) proposes a framework which is based on gain-based cache replacement policy named as Min-SAUD. This framework is for wireless data for dissemination when cache consistency is enforced before keeping the data to be put in cache. Their framework provides feature that effect cache performance, data size, update frequency, cache validation cost etc. They justify their result with simulation results which out-perform existing policies like LRU and SAIU.

(Chang, Y., K., et al, 2006) proposed a cache management framework in which dynamic web pages can be cached and managed in the mobile side just like in the server side in order to reduce the device's power consumption. Then, proposed IR-based approach which record 2 types of numbers that are updated web pages before and after their queries. They specified their results through experiments which projects 40-47% less power consumption.

(Kalim, U., et al, 2005) presented MAGI architecture which also addresses the issue of mobile offline processing when mobile device got disconnected from the network (either due to network failure or intentional disconnection). The web-services in the MAGI architecture make the development of architecture in such a manner that the

client does not have to connect with the proxy server throughout the time. They have done this mechanism with the help of notification operation type.

2.2.3(c). Summary of Data Cache Framework

Message management is very major and important mechanism for mobile devices in order to preserve the data message for future use while got disconnected. The cache of data message will be present in the device memory and hence make it faster to process. But the memory is not volatile medium so the data will get erased because of power failure. Therefore, the data message must of preserved on the hard disk, so it will not get effected even the mobile device run out of battery power failure. The data queue mechanism should be in mobile device as well as grid proxy server. This is one of the core contribution of this research work.

2.2.4. Security Architecture in mobile grid computing

2.2.4(a). Overview

The wireless network is not safe from malicious intruders, for these purpose different cryptography approaches and authentication mechanism like password-based, X.509 proxy certificate etc. is used for data integrity, confidentiality and security.

2.2.4(b). Cryptography approaches for mobile grid computing

There are many types of cryptography implemented in the mobile grid computing architecture in order to give solution of security issues arises in this paradigm. Some of these approaches are discussed briefly below:

1. Cryptography using Elliptic Curve Cryptography (ECC)
2. Cryptography using Public Key Infrastructure (PKI)

1. Cryptography using Elliptic Curve Cryptography (ECC)

(Jameel, H., et al, 2005) introduces framework employing the Web Service Security Model which gives secure communication access between mobile devices and the Grid itself. As opposed to RSA algorithm scheme for cryptography which requires heavy computation processing, their web service model supports multiple cryptography technologies that well suited for mobile device architecture. They mentioned in their work that the Elliptic Curve Cryptography (ECC) based public key scheme can be concatenated with the Advance Encryption Standard (AES) for the mobile access to the Grid. Although the key size is much smaller than that of RSA algorithm scheme, the security level is quite much equal.

(Tillich, S., and Großsch"adl, 2004) investigates the feasibility of the public key cryptography for mid to advance end mobile devices with specific to Elliptic Curve Cryptography (ECC). They have implemented and showed performance of J2ME enabled mobile devices with Elliptic Curve Digital Signature Algorithm (ECDSA) for signature generation and verification. They mentioned that all public key cryptography

requires higher processing power, resulting large amount of time for getting results in mobile devices. They get an average execution time of 20 seconds in the mobile devices but normally first execution cycle takes longer time. They compare the results of ECDSA and RSA which clearly shows the conclusion of their work. But their work is only suitable for PDA or smart phones.

2. Cryptography using Public Key Infrastructure (PKI)

In PKI architecture, it is assume that each entity have a pair of keys (i.e, private and public key). The private key is kept secret whereas public key is distributed among all nodes in the grid computing infrastructure. Introducing this GSI concept with respect to mobile device computing is bit challenging as well as difficult due to computational resource limitations of the mobile devices.

The proxy terms as a basis for an important feature that is single sign-on, which provides a mechanism to authenticate the user proxy. The proxy mutual authentication mechanism is slightly different in this respect that, the remote user not only gets the proxy certificate but also owner's certificate as well. The public key of an owner is used to validate the digital signature on the certificate while the CA's public key is used to authenticate the signature of the owner's certificate. Therefore, a chain of trust is been established between CA and the proxy (Lam, K., et al, 2004).

2.2.4(c). Secure Authorization mechanism in mobile grid computing

Different authorization mechanisms approaches were introduced and are used in the mobile grid computing architecture. Each of these approaches has their own positive and negative sides depending upon the infrastructure criteria.

1. Certificate-less Security Mechanism Architecture
2. Password-based Security Mechanism

1. Certificate-less Security Mechanism Architecture

Certificate-less enabled authentication is still used and widely popular because of ease of development and use for the end user. (Jo, S., et al, 2005) proposed a framework that is first mediated certificate-less public key encryption and signature schemes. Their framework follows the hierarchy structure and does not suffer from key escort property. In their work, they mentioned the mediate certificate-less public key cryptography (CL-PKI) will tackle the issues associated with the certificate management in the public key infrastructure (PKI).

(Chow, S., et al, 2006) also introduces a lightweight framework for security-mediated certificate-less (SMC) cryptography. This framework helps to maintain the mediation of the keys. They justify that they have avoid they key escort which is present in all the previous cryptography algorithms. Their work was the enhancement of Baek and Zheng 2004. Their framework uses same number of parameters for most the identity based and uses the same key generation center (KGC).

2. Password-based Security Mechanism Architecture

(Crampton, J., et al, 2007) proposed a security framework which uses password-based authentication and certificate-free GSI (PECF-GSI) for the grid application. Their architecture provides single sign-on feature without the use of public key infrastructure (PKI) and certificates. The important thing is that their architecture supports the essential security components like mutual authentication and delegation using public key infrastructure techniques. The mutual authentication and delegation doesn't require the public key certificates. In their work, they mentioned that this lightweight security framework is suitable for resource limited devices. Although, it lacks an important security component of authorization, but they mentioned that their future work will be related to it.

2.2.4(d). Summary of Security Architecture in mobile grid

Cryptography plays as important role making the data secure over a wireless network. Elliptic curve cryptography is a good cryptography approach but requires heavy computational power for cryptography process, hence not well suitable for the mobile devices. In the same way, PKI architecture is also secure but requires the public and private key manipulation along with the proxy certificates for the authentication and authorization mechanism. Traditional password-based authentication is considered to weak security level but does not require heavy computational process. It is difficult to have security, integrity and efficiency at the same time. But combination and

enhancement of any of above mentioned approaches can make a secure and efficient mobile grid computing architecture.

2.2.5. Network Infrastructure of Mobile Grid Computing

2.2.5(a). Overview

Ad hoc network is an infrastructure less network, which is formed by mobile devices like smart phones, laptop, PDA, TabletPC etc. As each device have its own computational capabilities, power, hardware resources, software configurations (OS, applications, protocol etc.), shares their computational resources with others, and hence forms the heterogeneous network. Specific to this thesis, the network infrastructure for mobile grid computing will be Mobile ad hoc network (MANET). Routing protocols in the MANET are often categorized by two divisions that are topology-based and position-based routing.

2.2.5(b). Review of Network Infrastructure in Mobile Grid Computing

In mobile ad hoc network (MANET), each node will act as a router which will be responsible for the maintaining the routes to the other nodes and connectivity in the network infrastructure. In this way, there is an element of co-ordination among the nodes. In this infrastructure, high end mobile device will share there resources to the devices with low resource. Thus, mobile ad hoc grid will help to make an interconnection of heterogeneous mobile devices to make a new service (Selvi, V. et al, 2007).

Developing middleware services especially for MANET is not an easy task. (Hadim, S., et al, 2004) conducted some survey regarding the methods and techniques which are based on the MANET architecture. In there survey report, they concentrate on the differences and the similarities of the different approaches of the MANET.

2.2.5(c). Summary of network infrastructure

The wireless network architecture of mobile grid computing is unstable and highly insecure. Due to instability of the network signals, mobile devices can be frequently disconnected. The network coverage area, data transmission rate and the signal stability depends on different wireless technology available such as Wi-Fi, Bluetooth etc. The secure layer can be achieved by implementing the cryptography mechanism.

2.2.3. Summary of Proxy-based Architecture

Many researchers proposed their framework regarding proxy server in a mobile grid computing architecture. But there are still some limitations and complexities which need to be address. Mobile device are limited in resources and computational power, so highly effective and efficient framework need to be proposed which give solutions regarding efficient cryptography for data integrity, effective data message recovery that is scalable as well as transparent.

2.3. Comparison of Proxy-based Architectures

Table 2.1, shows the some sets of attribute comparison of the Proxy-based architectures in mobile grid computing environment.

Table 2.1: Comparison of Proxy-based Architecture Frameworks

Features	LEECH	FINESSE	Proxy-based Grid Service	MAGI
Model Proposed by	(Phan, T., et al, 2002)	(Millard, D., et al, 2005)	(Guan, T., et al, 2005)	(Kalim, U., et al, 2005)
Authentication Mode from mobile to proxy	NO	NO	NO	NO
Adaptive Management by Offline Processing	NO	NO	YES	YES
Security layer between mobile and proxy node	NONE	NONE	NONE	Elliptic Curve + AES
Robust against Network Failure	NO	NO	YES	YES
Robust against Power Battery Failure	NO	NO	NO	NO

2.4. Summary

In this chapter, related work of mobile grid proxy architectures, cryptography of data security and authentication mechanisms along with the data cache management for data integrity is discussed briefly. In mobile proxy architecture, researchers tend to improve the framework in order to make it more secure and efficient. For data security, different cryptography approaches was mentioned, each had their own positive and

negative sides. Lastly, for data safety, different data cache management architecture was proposed so when mobile client gets disconnected the data will be safe and can be used later on.