A SURVEY ON SECURITY AND PRIVACY CHALLENGES IN MOBILE GRID COMPUTING

[1]Malwinder Kaur, [2]Mrs. Meenakshi Bansal
[1]M.Tech Student, [2]Assistant Professor,
Department of Computer Engineering,YCoE, Talwandi Sabo,
Punjabi University, Patiala.
Email: [1]malwinderkr2@gmail.com, [2]ermeenu10@gmail.com

Abstract - The security is essential for all the applications on network. For providing the security to many applications on the network, number of mechanism are used. Grid computing is believed to be ultimate solution for meeting the increasing computation needs of the organizations. At present major focus in Grid computing is to improve the performance of the grid. However, user running an application on a remote machine in the grid-computing network requires assurance about privacy and integrity of his data. Mobile Grid Computing(MGC) is the combination of Grid Computing and Mobile Networks to bring benefits for mobile users, network operators, as well as grid computing providers. Here we have to explore the security problems in grid computing and the steps that can be taken to solve them. The ultimate goal of MGC is to enable execution of rich mobile applications of mobile devices. The prominent feature of the MGC is the collaboration of multiple entities to perform collaborative tasks using mobile devices. Currently, most of the security solutions for mobile grid environment use static set of algorithms and protocols. The NTRU algorithm is concluded as a best and fast algorithm for providing security on the clouds. NTRU is a public key cryptosystem, which provides best security to cloud computing by encrypting and decrypting the data.

Keywords- Mobile Grid Computing, Authentication, Secure Communication, Android Platform, Encryption, Decryption, NTRU, AES and throughput

I. INTRODUCTION

Grid Computing

A Grid is a collection of heterogeneous computers and resources spread across multiple administrative domains with intent of providing users easy access to these resources. The major aim is to study about data grid security issues and provide solution to guard data or information in Grid Services that are appeared while operating in data storage systems and we present a cryptographic & fragment based scheme to accomplish the server protection requirements associated with a standard Data Grid environments.

The Data Grid is kind of distributed structure in which mutual assets (CPU or storage space) are offered. These surroundings likely to present the productive assets not only for processor - based jobs, but as well for the programs which need major sum of primary memory, physical memory space and network performance.

A high-level view of activities involved within a seamless, integrated computational and collaborative Grid environment is shown in Fig. 1.1

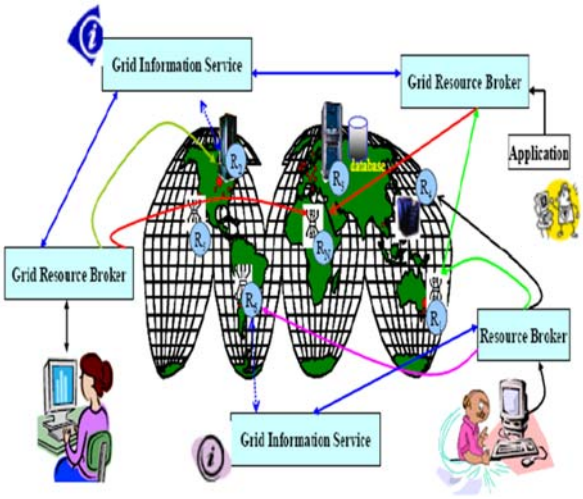

Fig. 1.1 A world-wide Grid computing environment

II. OVERVIEW OF MOBILE GRID COMPUTING

A. Defination of Mobile Grid

Mobile grid is a class of distributed systems, both wired and mobile, that autonomously engage in sharing of resources and exchange of services to provide higher performance and better utilization of the otherwise unutilized resources on the mobile devices. As the resources on the host are limited with power and memory constraints, it seems unnecessary for extending certain features of grid to the mobile host. But in future, when the systems become all-pervading, the constraints of power and memory would seem trivial when compared to the advantages offered by mobile grid. Besides, with continuous development in device technology, the constraints of power and memory are diminishing and mobile devices are having better specifications when compared to their predecessors. Mobile devices can make use of the available resources in the grid to perform any task or use them when on the move.

B. Mobile Grid Computing(MGC)

Mobile Grid computing extends traditional Grid computing paradigm to include a diverse collection of mobile devices that communicate using radio frequency, infrared, optical and the other wireless mechanisms. The prominent feature of mobile grid computing is collaboration of multiple entities to perform collaborative tasks using mobile devices that rely on two fundamental functions: communication and resource sharing. The fundamental function is to enrich one another and provide new solutions that solve many of limitations and problems found in different technologies, such as reduced CPU performance, limited secondary storage, heightened battery consumption sensitivity, and unreliable low band width communication.

Fig. 2.1 Mobile grid computing

In Fig 2.1 we have connected six low-end Android phones to create a mini-grid.

Security is a very important factor in mobile grid Computing and is also difficult to achieve owing to open nature of wireless networks and heterogeneous and distributed environments. Since Internet is not security oriented by design, there exist various threats, in the particular, malicious internal and external users. Securing communication and fine tuning controlling access to shared resources are the important issues for mobile grid services.

Currently, most of the security solutions for the mobile grid environment use a static set of algorithms and protocols. The countermeasures against threats utilize encryption/decryption for the confidentiality, the message authentication code for integrity, digital signature for authentication, undeniable digital signature for non-repudiation, access control for authorization, and intrusion detection/defense for availability/DOS. Here we try to explore the possibilities of using mobile devices like smart phones and tablets in the area of grid computing / distributed computing, talks about progress that has already been made in this direction and outlines techniques to be adopted for a successful implementation.

The main factors that hinder the growth of this paradigm as compared to the grid computing paradigm are the issues related to mobility and the constraints of mobile computing, mobile devices are poor in available resources as compare to wired systems, mobile devices are more prone to security breaches, mobile connectivity is highly variable in performance and reliability, mobile devices relay on a finite energy source.

C.Existing Mobile Grid Architectures

The architectures proposed have generally added up certain features to the existing grids so as to allow it to handle mobile devices. Many mobile grid infrastructures have been modeled in order to support mobile devices in the grid. One of the works in this direction was initiated by the European Union with the Akogrimo project. The base of the model was that of a service grid, as the mobile grid is based on its principles

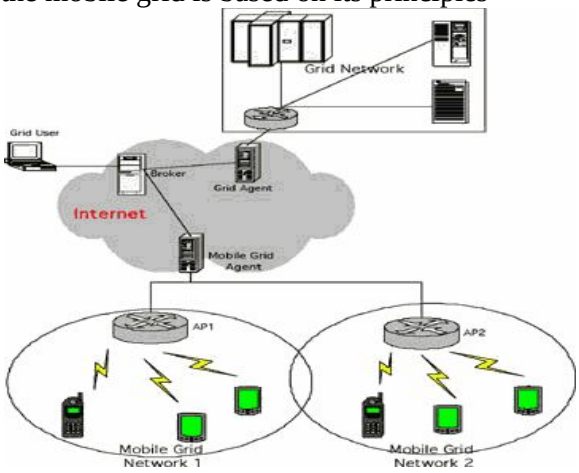

Fig.2.2 System architecture of mobile Grid system.

In Fig.2.2 it is described that mobile grid system which we are implementing is resource-sharing system using mobile agent technologies.

D. Need of Mobile Grid

Mobile Grid enables both the mobility of users requesting access to a fixed Grid and the resources that are themselves part of the Grid. Both cases have their own limitations and constraints that should be handled. In the first case the devices of the mobile users act as interfaces to the Grid enabling the job submission, monitoring and the management of the activities in an 'anytime, anywhere' mode, while the Grid provides them with high reliability, performance and the cost-efficiency.

E. Advantages of Mobile Grid

It is having following advantages:

a. Grids and mobile Grids can be ideal solution for many large scale applications having dynamic nature and require transparency for users.
b. Mobile grid will increase job throughput and performance of involved applications.
c. And will increase utilization rate of resources by applying efficient mechanisms for the resource management.
d. It will enable the advanced forms of the cooperative work by allowing the seamless integration of resources, data, services.
e. Mobile grid computing provides new technology for solving complex and compute intensive problems in mobile environments.
f. Mobile grid computing broadens the scope of grid computing by including a vast resource pool available in form of mobile devices.

F. Challenges

There are few important challenges that need to be addressed before this can be successfully adopted, of which primary challenges are: Power, Platform, Network and Social.

G. Applications that can take benefit from Mobile Grid Computing

a. The distributed wireless channel estimation.
b. The distributed target detection and tracking.
c. Estimation of the pollution level using real time air quality measurements and content based distributed search and sharing.

III. SECURITY CONCERNS IN MOBILE GRID

a. Mobile grid attracts many attacks due to its wide and open nature.
b. With the mobility, large distance inter-domain interactions between users increase and hence the security mechanisms must scale to a global level.
c. The mobility also adds the issue of physical security.
d. The wireless nature of network poses an additional threat.
e. The wireless network is more prone to eavesdropping, tracing and tampering of data.
f. Thus, means for secure handoff, managing disconnection etc. are needed to secure computing environment to prevent intruders & theft of resources.
g. Security in a mobile grid environment requires secure authentication and key management services along with the authorization, integrity and confidentiality.

IV. RELATED WORK

In literature review goes beyond the search for information and includes the identification and articulation of relationship between the literature and our field of research.

Begam and Mohamed [1], their work showed the focus to provide security and efficient power management. In this a framework of dynamic secure routing protocol called select successive hop routing(SSHR) algorithm using Abstract monitoring objects.(AMO) and Secure service certificate(SSC). It includes: Authentication of Mobile nodes, Security flow between Mobile devices and Saving battery power.

Gulmeher and Waheed [3], discussed that grid computing is a modern concept and it not just speedup computing and cut costs but causes a paradigm shift in computing. It adds security needs of both resource consumer and resource provider.

Gill *et al.* [2], described the study of N-Tier architecture, grid computing and its security issues.

By the study of NTRU it is concluded that it is fast and best for providing security.

Majithia and Singh [7], discussed the various algorithms used to secure data send by mobile phone using an android platform on network. It concluded that NTRU is faster and provide stronger security level than other traditional algorithms like DES(Data Encryption Standard) and RSA(Rivest-Shamir-Adleman).

V. OUTLINE OF ALGORITHMS

a. NTRU (Number Theory Research Unit) Algorithm

NTRU cryptosystem is a relatively new Public Key Cryptosystem. Public Key Cryptography or Asymmetric Cryptography is used in areas of digital signatures and key exchange. RSA is an acclaimed Public Key cryptosystem that is in use since 1977. However, it is very slow in comparison with Symmetric Cryptography systems in processing bulk data encryption and decryption. In contrast, NTRU runs much faster on large data systems than RSA and has become a very popular algorithm today in terms of data encryption and decryption. The key generation process in NTRU is much faster than that in RSA and this process is one of the most important processes in Public Key Cryptography.

NTRU Public Key Cryptosystem

Public-Key Cryptosystem, named NTRU stands for Number Theorist Research Unit. NTRU is ring-based cryptosystem. NTRU was set up in 1996 and turned in to an absolutely efficient company in 2000. NTRU was recently taken over by Security Innovation, an application security company. NTRU is comparatively a new cryptography technique that is known to be more proficient than the existing and more extensively used public-key cryptosystem like RSA.

-Key generation

NTRU involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

-Encryption

-Decryption

NTRU is better than all other algorithms in throughput and power consumption.

Features	**NTRU**	**DES**	**RSA**
Approach	A-symmetric	Symmetric	A-symmetric
Encryption Time	Low	Moderate	High
Decryption Time	Low	Moderate	High
Throughput	High	Moderate	Low
Power Consumption	Low	Moderate	High
Confidential	High	Moderate	Low

Table 5.1 Distinction between NTRU, DES and RSA Algorithms[7].

b. AES (Advanced Encryption Standard) Algorithm

In 1997, NIST initiated a very public, process to develop a new secure cryptosystem for U.S. government applications. The result of the Advanced Encryption Standard, became official successor to DES in December 2001. The AES uses an SKC scheme called Rijndael, block cipher designed by Belgian cryptographers Joan Daemen and Vincent Rijmen. Algorithm can use a variable block length and key length; the latest specification allowed any combination of keys lengths of 128, 192, or 256 bits & blocks of lengthof 128, 192 or 256 bits.

(i) Do the following one-time initialization process:

(a) Expand the 16-byte key to get actual key block to be used.
(b) Do the one time initialization of 16-byte plain text block.
(c) XOR the state with the key block.

(ii) For each round, do the following:

(a) Apply S-box to each of plain text bytes.
(b) Rotate row k of plain text block by k bytes.
(c) Perform a mix columns operation.
(d) XOR the state with the key block.

VI. CLIENT SERVER COMPUTING IN MOBILE ENVIRNMENT

Advances in wireless networking technology and portable information appliances have engendered a new paradigm of computing, called *mobile computing*, in which users who carry portable devices have access to information services through a shared infrastructure, regardless of their physical location or movement behavior. Such a new environment introduces new technical challenges in the area of information access. Traditional techniques for information access are based on the assumptions that the location of hosts in distributed systems does not change and the connection among hosts also does not change during the computation. In a mobile environment, however, these assumptions are rarely valid or appropriate. Mobile computing is distinguished from classical, fixed-connection computing due to :
(1) the mobility of nomadic users and their computers (2) the mobile resource constraints such as limited wireless bandwidth and limited battery life.

The mobility of nomadic users implies that the users might connect from different access points through wireless links and might want to stay connected while on the move, despite possible intermittent disconnection. In a mobile client-server information system, a loose or tight collection of trusted information servers are connected via a fixed network to provide information services to a much larger collection of untrusted mobile clients over wireless and mobile networks.

Paradigms of Mobile Client-Server Computing

In this section, we briefly examine the impacts of mobility on information services and applications, and the new paradigms of client-server computing needed to deal with these impacts. A categorization of these computing paradigms is given below. This examination should facilitate our analysis and review of the various proposed techniques for mobile information access. Existing research on mobile client server computing can be categorized into the following three paradigms:

(1)Mobile-aware Adaptation: The paradigm of mobile-aware adaptation covers various strategies and techniques in how systems and applications respond to the environmental changes and the resource requirements. It also suggests the necessary system services that could be utilized by mobile-aware applications.

(2)Extended Client-Server Model: The extended client-server model facilitates mobile client-server information access. One distinguishing feature is the dynamic partitioning of client-server functionality and responsibilities. The extended client-server model provides a way to support the adaptation of mobile systems and applications. The paradigm of the extended client-server model includes various client-server computing architectures that enable the functional partitioning of applications between clients and servers.

(3)Mobile Data Access: Mobile data access addresses issues such as how server data can be delivered to client hosts, how data over wireless and mobile networks is structured, and how the consistency of client cache is ensured effectively. The adaptive strategies for mobile data access depend largely on the type of communication links, the connectivity of mobile hosts, and the consistency requirements of applications. In our view, mobile data access provides another way to characterize the impact of mobile computing constraints on information access.

Extended client-server model

Another way to characterize the client server computing in mobile environments is to examine the effect of mobility on the client-server computing model. In a client-server information system, a server is any machine that holds a complete copy of one or more databases. A client is able to access data residing on any server with which it can communicate. Classic client-server systems assume that the location of client and server hosts does not change and the connection among them also does not change. As a result, the functionality between client and server is statically partitioned. In a mobile environment, however, the distinction between clients and

servers may have to be temporarily blurred resulting in an *extended client server model* shown in Figure 6.1. The resource limitations of clients may require certain operations normally performed on clients to be performed on resource-rich servers.

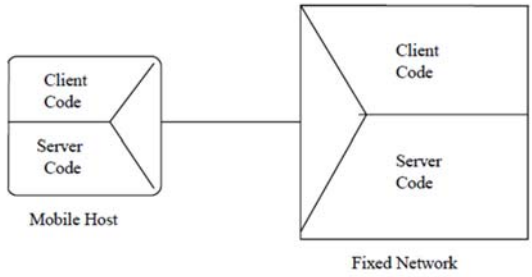

Fig. 6.1 Extended Client-Server model

Flexible Client-Server Architecture

Flexible client-server architecture generalizes both thin client and full client architectures in that the roles of clients and servers and application logic can be dynamically relocated and performed on mobile and stationary hosts (see Figure 10). In the flexible architecture, the distinction between clients and servers may be temporarily blurred for purposes of performance and availability. Furthermore, the connection between clients and servers can be dynamically established during the execution of applications.

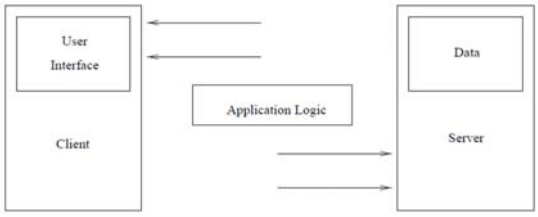

Fig. 6.2 A flexible Client- Server computing

VII. CONCLUSION

Data has become more important as the methods which are used to ensure security not only need to be strong and efficient but should be easy to implement and execute. Grid computing is a modern concept that not just speeds up computing and cut costs. However, several challenges still weigh down the technology. Resolving security problems with grid computing is one such major challenge. It requires an adequate understanding of both the security issues in grid computing implementation as well as the solutions presently available to address these. This system addresses the security needs of both resource consumer and resource provider. The security model is used to improve security without degrading the performance of the system. Main goal of future improvement is provide more security by using more secure algorithm whose security can't be broken. Second goal is to reduce encryption and decryption time to process data.

ACKNOWLEDGEMENT

I express my sincere gratitude to my guide **Mrs. Meenakshi Bansal** (Assistant Professor, GKC, Talwandi Sabo), for his valuable guidance and advice. Also I would like to thanks all the faculty members and colleagues for their continuous support and encouragement and a special acknowledgement to the authors of various research papers and books which help me a lot.

REFERENCES

[1]. Begam, P. and Mohamed, M., (2013), "ASAMO: Authentication and Secure Communication using Abstract Monitoring Objects for Mobile Grid Computing", *International Conference on Informatics and Creative Multimedia.*

[2]. Gill, A.K.**,**(2014), " Security of N-Tier Architecture using NTRU", *International Journal of Advanced Research in Computer Science and Software Engineering,*4(7).

[3]. Gulmeher, R. and Waheed, M.A., (2014), " Security Analysis for Data Grid Middle wares", *International Journal of Advanced Research in Computer Science and Software Engineering,*4(5).

[4]. Kathrine,G.J.W.,(2011), "A Novel Security Framework for Computational Grid", *In the Proceedings of IEEE.*

[5]. Kumari, A., (2011), "Grid Based Security Framework for Online Trading", I*n the Proceedings of IEEE.*

[6]. Lonea, A.M. and Popescu, D.E., (2010), "Security Issues For GRID Systems", *In the Proceedings of IEEE.*

[7]. Majithia, S. and Singh, S., (2013), " Implementation of NTRU on Cloud Network in an Android Platform and Comparison with DES and RSA", *International Journal of Advanced Research in Computer Science and Software Engineering,3(11).*

[8]. Mishra, N.,(2014), "SECURITY ISSUES IN GRID COMPUTING", *International Journal on Computational Sciences & Applications (IJCSA),4(1).*

[9]. Mote, Y., (2012), "Superior Security Data Encryption Algorithm(NTRU)", *An International Journal of Engineering Sciences, 6(12).*

[10]. Mukhin, V., (2007), "The Security Mechanisms for Grid Computers", *IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.*

[11]. Ranjan, R., (2012), " Improvement of NTRU Cryptosystem" , *International Journal of Advanced Research in Computer Science and Software Engineering,2(9).*

[12]. Pardeshi, S.,(2013), "Grid Computing Architecture and Benefits", *International Journal of Scientific and Research Publication,3(8).*

[13]. Hashemi, S. and Bardsiri, A., (2012), "Cloud Computing Vs. Grid Computimg", ARPN Journal of System and Software, 2(5).

[14]. Zeng, W.,(2008), "Mobile Grid Architecture and Application", *In the Proceedings of IEEE.*