# Grid Computing Security Implementation Challenges

**Muhammad Naeem khan, Shahid Hussain**

Department of Computer Sciences, Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology Islamabad, Pakistan
Muhammad Ibrahim {E-Lecturer Virtual University Islamabad Campus}

**Abstract**
Grid networks are today's more focusing area of research for the researchers due to the services it provides with its cost effectiveness in the most advanced technologies in an innovative use. Even though it is providing various level of services, still it is facing very big challenges, due to the security concerns, that may arise in a collaborative environment for creating a level of trust among the organization that will be part of the grid. This paper will review the literature of the work done in past and currently for tackling the security concerns and will lay a foundation for making the security and privacy more tighten in such a large collaborative environment that can grow to a very large scale. This work will mainly focus on the current trends in grid network for coping with the security and privacy issues.

***Keywords:***
*Grid Security, virtual organization (VO), privacy, authorization, authentication, OGSA.*

## 1. introduction

The Grid system is a scalable and autonomous infrastructure which manly concerned with the integration, virtualization and management of services and resources in a distributed, heterogeneous environment that support collections of users and resources (Virtual Organizations) across traditional administrative and different organizational domains. Grid is a large scale resource sharing and distributed computing environment that couples thousands of computers, storage systems, networks, scientific instruments and other devices distributed over heterogeneous wide area networks [5]. Due to the grid system we could be able to connect to different organizations and able to use their resources. Due to the use of grid system, an organization is able to reduce their hardware cost and also if its need high computations by using grid they are also able to use the resources under multiple domains. So because of that it's create a lot of security challenges e.g. authentication, authorization and dynamic trust relationship across different domains. For such problems different security techniques are used e.g. WS-security specifications. etc. this is currently the foundations of any security solutions for both Web services and grid services applications.

In this work my main focus on the security issues like authentication, authorization, single logon in the grid environment e.g. when two cross organizations communicate with each other, how to make this communication secure fast by regarding their local security mechanisms.

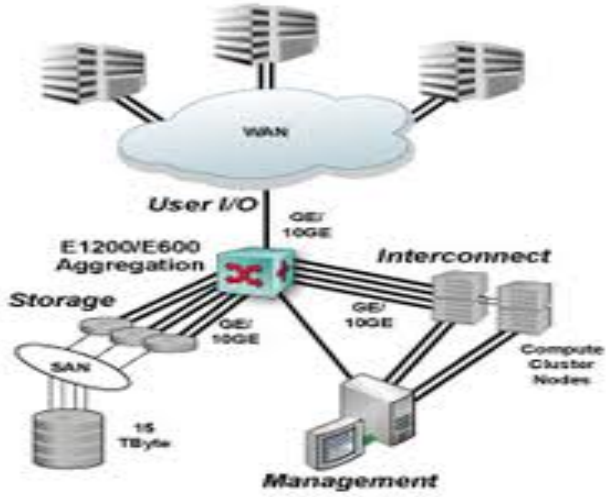


Figure 1: grid architecture

## 2. literature Review

In grid architecture the dynamic trust is the most important in cross organizational authentication. In this paper [1] the authors Mehran et al have presented architecture for credential mapping to overcome the heterogeneity problem in different organizations. By using the credential mapping mechanism it is possible to make dynamic and fast trust relationship between the cross organizations regardless of their local security mechanism. In the paper the work presented is only deals with the authentication tokens.
The strength of the paper is that, the credential mapping mechanism is more secure and fast for the dynamic trust between the cross organizations. The developed mechanism is lightweight, easy to integrate and open source service for grids. Limitation of the paper is that it only deals with the authentication token mapping not with the authorization and attribute mapping.
In this paper [2] the authors zhang et al proposed a layered model and several security services for built a secure grid service [2]. The papers discuss the security model to

Manuscript received February 5, 2013
Manuscript revised February 20, 2013

provide security for grid services. The approach is very much efficient in the sense that authentication and authorization is tackled at different layers. Strength of the paper is that, is that service requestor is discovered by the policies dynamically and make decisions at runtime, which is more suitable in a dynamic environment like grid [2]. One of the best functionality of this model is that authorizations is performed locally and have thus level of access and the authentication mechanism is treated different based on the authorization level. The limitation of the paper is that they only focused on security of grid environment and given no attention to the performance issue of grid systems.

In this paper [3] the authors Zha et al proposed a security framework for the china national grid. In this framework for the authentication process they used the digital signatures, and proposed that in this environment each user and resource must have a certificate which contains information about the user or resource. For the implementation of their idea they introduce the concept of "Agora", the main theme of Agora is to group each user and resource according their needs and policies [3]. The Agora contains entries for each user and resource which comprise them into several groups. For the secure communication and data integrity between different resources and users they used the concept of SOAP messages. The strength of the paper is that the authentication is performed using digital signatures and authorization decision is made based on the local mechanism of access level of the virtual organization and resource availability for the communication across the grid. The limitation of this paper is that the method is very costly.

In this paper [4] the author has proposed a mechanism for service provisioning across the grid in service oriented architecture, using GT3's security architecture intact. The trust is formed across the grid nodes of different Virtual Organizations, distributed across diverse locations having different local security mechanism, without the need for much privileged network service [4]. The strength of this paper is that this model is very much flexible in terms of coping with the trust across different VO, using a very effective and least-privileged model for credential exchange. The limitation of this paper is that as it uses web standards so still some of the web services are in standard process that will create some problem in implementing the proposed model for some of the web services for giving grid services using web services

In this paper [5] the author's sarbjeet et al proposed a framework model for the grid security services. This framework model is composed of different layers in which each layer is concern with different security measures. The strength of the paper is that the proposed model deals with the security both in general and on application level [5]. It hides the details of the local security mechanism to the requester of another virtual organization, for accessing the service across the grid. The limitation of the work is that the ideas are not supported with implementation. No validation is performed to validate their ideas they have presented in this paper. The framework also does not deal with the authentication and authorization process.

In this paper [6] the author's wenjie et al proposes a secure structure for the grid environment. The proposed structure not only able to provide secure communication between different hosts and resources, but also responsible for the fault tolerance and recovery from the fault. This structure has different level of security in which each layer is responsible for a specific task.

The strength of the paper is that they cover both the secure communication as will as the fault recovery problem of the grid environment. The limitation of the paper is that they did not perform any validation to validate their ideas they have presented in this paper

In this paper [7] the author's Azadeh et al proposed a model which based on the message level security. The proposed model based on the evolutionary approach for creating secure grid services. They used the WS-security techniques for their idea. They show a mechanism for the client to provide authenticated data and also for the service to receive data. It uses a mechanism for the client to provide authentication data and for the service provider to retrieve those data. The strength of the paper is that it uses XML Digital Signatures and encryption to achieve a level of trust by used of certificates that were issued by CAs [7]. The limitation of the paper is that they do not performed simulation to validate their ideas.

In this paper [8] the author's Geethakumari et al proposed a model for the grid system and security needs for the grid environment by the name of FTDM (fuzzy trusted and delegation model) for the access control. They used the idea of delegation for the authorization process in case of indirect access to the resource in virtual organization. The delegation has two types that is static and dynamic delegation. In static delegation everything is predefined while in case of dynamic delegation a dynamic trust is required for both the users in virtual organization. The strength of the paper is that material provided in the paper is fully support their idea. The limitation of the paper is that the model represented does not have the actual implementation in the real grid environment.

n this paper [9] the author Vadym proposed an OGSA (open grid service architecture) for the grid environment. He point out some of the challenges and requirements for the existing OGSA model and on the basis of these requirements, the author proposed some techniques which based on the existing technologies. The strength of the paper is that he used standard techniques which are already approved to overcome the requirements of the OGSA.

The limitation of the paper is that they do not performed simulation to validate their ideas.

In this paper [10] the author's Yuri et al does not proposed any new idea or model for the grid architecture. They just

study out the existing security models i.e. OGSA etc and point out the weaknesses of these models. They proposed some new research area's related to grid security on the bases of the models. According to the paper if we workout on such area's point out by the author's, than we could be able to build a secure grid system. The author has analyzed several currently deployed Grid security systems and architectures in his work we have attempted to and indicated the limits of their applicability. The limitation of the paper is that they do not have any solid process which can able to prove their new idea's which they proposed.

In this paper [11] the author's Prasanna et al proposed a new idea for the high performance and secures communication in grid environment. They introduce the concept of load sharing for faster communication. For this purpose when two nodes needs to communication they simply select an ADM (authentication distribution managers) and hands over it, the security policies. The ADM then select other idles nodes in the system and share the security implementation load with them. So by this we can be able to assure higher performance. The strength of the paper is that, the idea is very simple and gives very good performance keeping the security tight. The limitation of the paper is that, they haven't done simulation to validate their work. The implementation would be costly. It is also possible that when there is no free node that can act as ADM then this model will not give efficient results.

In this paper [12] the author's Chen et al proposed a reflective authentication framework for the china national grid. The proposed model consists of the three main components, meta-model, meta-data and meta-protocols. The meta-model is user visible, it simply the interface for the user to send his authentication ID The meta-data is the collection of software modules, while the meta-protocols are the rules for the communication across the grids.

Strength of the paper is that, the model is very lightweight and cheap. The limitation of the paper is that, they only focus on authentication process and not concern with the authorization and performance of the system.

In this paper [13] the author's MingChu et al work on the OGSA model and point out some drawbacks of the architecture. On the base of these drawbacks, they suggest that the grid system needs a more secure architecture than the existing one. For this purpose they proposed a new architecture for the grid security. They compare the two models and claim that their new architecture is better than the OGSA model.

The strength of the paper is that, they used standard techniques which are already approved to overcome the requirements of the OGSA.

Limitation of the paper is that, they do not validate their idea through simulations. They also not explain that how will be the authentication and authorization made in the system.

## 3. Critical analysis

TABLE 1

| Author | Working | Problems | Solution |
|---|---|---|---|
| Mehran et al | Credential mapping mechanism for creating dynamic trust is very fast easy to integrate, lightweight for grid environment. | The mechanism presented in this is very will for dynamic trust but, it's only deals with the authentication token mapping not with the authorization and attribute mapping. | Work should be done in authorization level for efficient level of access to the users that require some level of service. |
| zhang et al | The layer model proposed in this work provides functionality for the authorization and authentication. | In this work the authorization is done at local, but they only focus on the authorization and authentication and does not deal with performance. | The authentication and authorization mechanism should be made efficient for giving level of access to the user based on their requirements and priority levels that can increase that can performance of the grid network. |
| Zha et al | In this work they use digital signature for the authentication of the user cross the grid. | The idea proposed is very will for the authentication across the grid but it is very costly. | The idea is very good for grid system but if we able to make it cheap |
| Von Welch et al | The used GT's grid architecture and provide mechanism for dealing with locally security | The model is very much flexible in terms of coping with the trust across different VO, using a very effective and least-privileged | If the same idea is used for the grid security services. |

| | | | |
|---|---|---|---|
| | mechanism. | model for credential exchange. But they deals with web security services. | |
| Sarbjeet et al | The proposed model deals with the security both in general and on application level. It hides the details of the local security mechanism to the requester of another virtual organization, for accessing the service across the grid. | The idea is will suited for the grid environment but No validation is performed to validate their ideas they have presented in this paper. The framework also does not deal with the authentication and authorization process. | They only focus on communication process does not concern about authorization and authentication if this functionality is added to this model. |
| Wenjie et al | The work presented in this paper is deals with both the security issues that may arise during communication and fault recovery problem of the grid environment. | The mechanism proposed for coping with the security and privacy issues is suitable for dynamic environment like grid. The fault recovery mechanism is used for in some situations however the results are not efficient for most of the heterogeneous environments for fault tolerance, which is the basis need of a grid networks. | A new mechanism is required for the fault tolerance across the grid network that can help in a heterogeneous environment. |
| Azadeh et al | The model proposed in this work is based on the message level security by following an evolutionary approach. | They used XML Digital Signatures and encryption to achieve message level security. The author did not come with simulating their model to validate their idea. | The idea is very suitable but if it is validated for a particular environment using simulation to check the results |
| Geethakumari et al | The author has proposed an idea which is based on the delegation of rights to the users based on their level of access and the requirements for creating trust across grid. | The material provided in the paper is fully support their idea but the author hasn't shown any validation of the proposed model using simulation. | It would be a good idea to have mechanism to separate different users in to different groups based on their level of access and priority level and then use the delegation technique for giving services to the users. |
| Vadym et al | The author proposed new ideas for the current models of security for the grid. | The idea proposed used standard techniques which are already approved to overcome the requirements of the OGSA. But is does not have any simulation for the idea. | If some work is done on the implementing this idea in the grid environment, for checking its results would give a chance to compare it with other techniques used for tackling the security and privacy issues. |
| Yuri et al | The authors reconsider the OGSA model and point out its security issues and proposed some new ideas for the security. | The author used standard techniques which are already approved to overcome the requirements of the OGSA.but they do not performed simulation | If some work is done on the implementing this idea in the grid environment, for checking its results would give a chance to compare it with other techniques used for tackling the security and |

| | | | |
|---|---|---|---|
| | | to validate their ideas. | privacy issues. |
| Prasanna et al | The author introduces the idea of load sharing for the fast performance and secure communication in the grid environment. | The idea is very simple and gives very good performance keeping the security tight but, they haven't done simulation to validate their work. Also implementation would be costly. It is also possible that when there is no free node that can act as ADM then this model will not give efficient results. | One solution is that if we select a master system as a permanent ADM that will provide the security service. |
| Chen et al | In this they proposed a reflective authentication model for china national grid. Which mainly concern with the authentication process of the grid networks. | In this paper the proposed model is very lightweight and cheap. But They only focus on authentication process and not concern with the authorization and performance of the system. | Enhancement should be made so that the model can consider the Authorization keeping in view the performance issues of the system. |
| MingChu et al | In this work the author's point out the weaknesses of the OGSA model and say that grid computing needs more secure model then the OGSA. They proposed their own model for the grid network. | In this work the author's used standard techniques which are already approved to overcome the requirements of the OGSA. But they do not validate their idea through simulations. They also not explain that how will be the authentication and authorization made in the system. | The idea is good but it need further improvement to increase the performance and to developed mechanism for the authentication and authorization. |

## 4. CONCLUSION

This work has reviewed the current and past trends for tackling the security concerns and has shown the solution for making the security and privacy more tighten in such a large collaborative environment that can grow to a very large scale. A comprehensive threat analysis is done regarding the security of grid architecture. The work has discussed various methods for creating dynamic trust and level of access to the users based on their needs with different methods for security that include with and without having taking care of the local security policies of the organization that is a part of the grid network.

## 5. FUTURE WORK

Future work includes developing a security model for the tackling the security and creating a dynamic trust among the VO across the grid, and have a tight least privilege model with no requirements for the user to be aware of the local security policies from where it is to be served. As the current security technologies do not meet the requirements of the grid environment as expected, therefore the current technologies needs to be updated.

## References


[1] Mehran Ahsant, Esteban Talavera Gonz´ alez, Jim Basney "Security Credential Mapping in Grids" International Conference on Availability, Reliability and Security IEEE 2009

[2] Zhongping Zhang Kunbo Wang Jianfeng Luan" A Combined Grid Security Approach Based on Web Services Security Specifications" ISECS International Colloquium on Computing, Communication, Control, and Management IEEE 2008

[3] Lin YU, Li Zha, Xiaoning Wang, Haojie Zhou, Yongqiang Zou., "GOS security: design and implementation "2009 15th International Conference on Parallel and Distributed Systems

[4] Von Welch, Frank Siebenlist, Ian Foster John Bresnahan Karl, Czajkowski, Jarek Gawor Carl Kesselman, Sam Meder ,Laura Pearlman, Steven Tuecke" Security for Grid Services" International Symposium on High Performance Distributed Computing, IEEE 2003

[5] Sarbjeet Singh, Seema Bawa "Design of a Framework for Handling Security Issues in Grids" international conference on information technology IEEE 2007"

[6] LIU wenjie, GU guochang," security issues in grid environment" International Conference on Services Computing IEEE 2004

[7] Arya Iranmehr, Arya Iranmehr, Mohammad bagher Sharifnia "Message-Based Security Model for Grid Services, Second

International Conference on Computer and Electrical Engineering" IEEE2009.

[8] G Geethakumari, Atul Negi, V N Sastry "Dynamic Delegation Approach for Access Control in Grids" First International Conference on e-Science and Grid Computing IEEE 2005.

[9] Vadym Mukhin "The Security Mechanisms for Grid Computers" International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IEEE 2007, Dortmund, Germany

[10] Yuri Demchenko, Cees de Laat, Oscar Koeroo, David Groep NIKHEF " Re-thinking Grid Security Architecture" Fourth IEEE International Conference on eScience. IEEE 2008

[11] Jingshu Chen1, Hong Wu1, Qingyang Wang1, Qingguan Wang1, Xuebin Chi "A Reflective Framework for Authentication in Grid Computing Environments" 5th international conference on grid and cooperative computing IEEE 2006.

[12] V.Prasanna Venkatesh, V.Sugavanan "high performance grid computing and security through load balancing" International Conference on Computer Engineering and Technology IEEE 2009.

[13] MingChu Li, Yongrui Cui, Yuan Tian "A New Architecture of Grid Security System Construction" International Conference on Parallel Processing Workshops IEEE 2006.