The Grid Authentication System for Mobile Grid Environment

A.Sudha[1] S.M.Karpagavalli[2] Chamundesshwari[3]
[1, 2]Computer Science And Engineering Department
[3]Electronics and Communication Engineering
[1, 2, 3]Al-Ameen Engineering College Erode

Abstract--- Grid computing is the major resource environment. Security and authentication is the important factor in the grid environment. Recently, Authentication protocol has been recognized as an important factor for grid computing security. This system proposes a new simple and efficient Grid authentication technique providing user anonymity. The system is based on hash function, and mobile users only do symmetric encryption and decryption. In this system, it takes only one round of messages exchange between the mobile user and the visited network, and one round of message exchange between the visited network and the corresponding home network. The system is designed as three applications such as authentication server terminal proxy and grid node. The grid user application is designed to handle user management and authentication process. The terminal proxy is an intermediate application to carry out authentication under the current coverage. The grid node application is designed to communicate the authentication server and terminal proxy with mobility operations. The user id, password and session key values are used for the authentication process. The proposed architecture possesses several desirable emerging properties that enable it to provide an improved level of security for grid computing systems. The one way hash function and time stamp mechanisms are used to perform the user authentication operation under the home network and visited network environment.

Keywords: security,hash function,encryption,decryption

I. INTRODUCTION

Grid computing came into existence as a manner of sharing heavy computational loads among multiple computers to be able to compute highly complex mathematical problems. However, it developed rapidly into a way of sharing virtually any resource that is available on any machine on the grid. Wired grids are now used to share not only computing power, but also hard disk space, data, and applications. The grid topology is highly flexible and easily scalable, allowing users to join and leave the grid without the hassle of time and resource hungry identification procedures, having to adjust their devices or install additional software on them. When it comes to computational grids, some old challenges that have always existed in the realm of computing security still remain. Security is always a balance of vulnerabilities and threats. “Grid” is a type of parallel and distributed system that enables the sharing, selection, and aggregation of geographically distributed "autonomous" resources dynamically at runtime depending on their availability, capability, performance, cost, and users' quality-of-service requirements Grids can be used to harness computational horsepower, provide access to unified data, or other intensive tasks. From a security manager's viewpoint, a corporate grid represents a high-value target for anyone who would want to gain unauthorized access. They need to be protected not only because they are high-value assets representing lots of hardware and software, but because they often serve a strategic function that's central to success. At the same time, security managers understand that successful security is about tradeoffs. Tighten security too much, and it'll become harder for the R&D folks to share their findings with Engineering. Make it too hard to share information, and pretty soon all kinds of ad-hoc systems will start popping up that provide back doors to the system. The growing popularity of the Internet along with the availability of powerful computers and high-speed networks as low-cost commodity components are helping to change the way to do computing. These new technologies are enabling the coupling of a wide variety of geographically distributed resources, such as parallel supercomputers, storage systems, data sources, and special devices, that can then be used as a unified resource and thus form what is popularly known as the “Grids”. The Grid is analogous to the power (electricity) grid and aims to couple distributed resources and offer consistent and inexpensive access to these resources irrespective of their physical location.fig 1.1 shows the grid view.

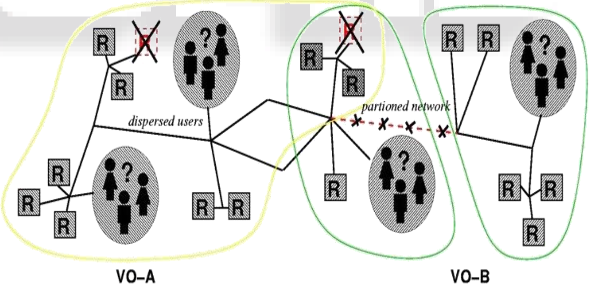


Fig. 1: Global view of grid services

A. Grid Computing and wireless techonolgy

Grid computing came into existence as a manner of sharing heavy computational loads among multiple computers to be able to compute highly complex mathematical problems. However, it developed rapidly into a way of sharing virtually any resource that is available on any machine on the grid. Wired grids are now used to share not only computing power, but also hard disk space, data, and applications. The grid topology is highly flexible and easily scalable, allowing users to join and leave the grid without the hassle of time and resource hungry identification procedures, having to adjust their devices or install additional software on them. The goal of grid computing is described as "to provide flexible, secure and coordinated resource sharing among dynamic collections of individuals, institutions and resources”. It is intended to be a dynamic network without geographical, political, or cultural boundaries that offers real-time access to heterogeneous resources and still offer the same characteristics of the traditional distributed networks that are in use everywhere in houses and offices. These characteristics being stability, scalability, and flexibility as the most important ones. Ian Foster offers a checklist for recognizing a grid.

A grid allows:

- Coordination of resources that are not subject to centralized control
- Use of standard, open, general-purpose protocols and interfaces
- Delivery of nontrivial qualities of service

B. *Wireless Grid*

One of the biggest limitations of the wired grid is that users are forced to be in a fixed location as the devices they use are to be hard wired to the grid at all times. This also has a negative influence on the flexibility and scalability of the grid; devices can only join the grid in locations where the possibility exists to physically connect the device to the grid. One description of the wireless grid is "an augmentation of a wired grid that facilitates the exchange of information and the interaction between heterogeneous wireless devices" Argawal, Norman & Gupta identify three forces that drive the development of the wireless grid

II. PROBLEM DESCRIPTION

A. *Existing System*

The use of a user's identity as the basis for delegation in distributed systems has venerable roots in existing security practice. However, it is the fundamental source of the cited scalability and flexibility problems. To solve these issues requires an acceptance that in very large distributed systems it will be impossible to base authorization on individual user identity: the security policy for any given machine must not require a list of all possible remote users. It is straightforward to group users into roles; remote processing can then be authorized on behalf of groups. An individual user's session can be given temporary authority by an authorization service acting for the group and individual accountability can still be traced via a session pseudonym. Remote machines need only to associate privileges with temporary accounts assigned to the group. It can deal with some of the issues: user names are managed locally, providing more flexibility in forming and changing groups, sessions are identified pseudonymously enhancing the prospect of privacy.

Grid security infrastructure (GSI) in Globus Toolkit uses PKI technologies to handle authentication, single sign-on, and trust delegation. However, it is not capable of assessing local security condition in a Grid site. The proposed trust model is aim to assess local security conditions to match with dynamically changed job security demands. The System introduce the trust index of a Grid site, which is determined by site reputation and self-defense capability attributed to the site track record, risk conditions, hardware and software defenses deployed at a Grid site.

B. *Proposed System*

When it comes to computational grids, some old challenges that have always existed in the realm of computing security still remain. Security is always a balance of vulnerabilities and threats.. Grids can be used to harness computational horsepower, provide access to unified data, or other intensive tasks. From a security manager's viewpoint, a corporate grid represents a high-value target for anyone who would want to gain unauthorized access. They need to be protected not only because they are high-value assets representing lots of hardware and software, but because they often serve a strategic function that's central to success. At the same time, security managers understand that successful security is about tradeoffs. Tighten security too much, and it'll become harder for the R&D folks to share their findings with Engineering. Make it too hard to share information, and pretty soon all kinds of ad-hoc systems will start popping up that provide back doors to the system.

III. SYSTEM IMPLEMENTATION

A. *Module Description*

The grid authentication system for mobile grid environment is developed to provide authentication feature for the grid clients. The grid nodes are connected from one coverage area and visited to different coverage areas. The authentication process is carried at at each coverage area. The node mobility and authentication process are the important functions of the system. The time stamping concept, one way hash function and Advanced Encryption Standard (AES) algorithm are used in this system. The system is developed with Java language and Oracle back end. The system is developed as three major applications. They are grid authentication server, terminal proxy and grid node or terminal operator.

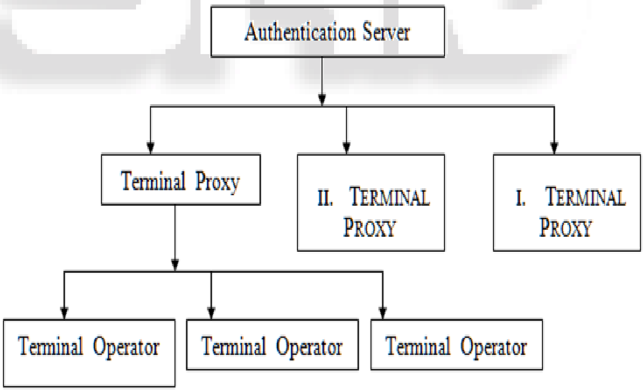


Fig. 2: system architecture

The grid authentication server application is designed to handle the user management and authentication process. The terminal proxy applications are also monitored by the grid authentication server. The terminal proxy application is designed to authenticate and monitor the monitor the mobility of the terminal operators. Session key management is also performed at the terminal proxy environment. The terminal operator or grid node is the end user application that share resource among the grid environment. The authentication server, terminal proxy and terminal operator applications are designed with pull down menu options. Each menu option is connected with an input or output form. The input forms are designed with data validation process. The application can be connected from cross platform environment. The Remote Method Invocation techniques are used for the communication process. The terminal proxy applications are connected with the grid authentication server. The terminal operators are connected with terminal proxy application. The terminal operators can be moved from one coverage area to another with reference to the terminal proxy applications.

B. *Grid Authentication Server*

The grid authentication server application is the top level application in this system. Terminal operator authentication and terminal proxy monitoring are the main operations of the grid authentication server. It is an administrator for the mobile grid environment. The grid authentication server also maintains the user registration process. The server application is divided into three major modules. They are users, terminal proxy and authentication modules. The users module is proposed to maintain the users. The terminal proxy module is designed to monitor the terminal proxy application. The authentication module is designed to carry out the authentication request and maintain the user logs.The users module is divided into three sub modules. They are user register, user management and authorized users. The user register sub module is designed to register new users. The user id, user name, password and user description are stored in the database. All the user details are maintained in the Oracle database. The user management is designed to handle the user modify, user delete and user list operations. The user list shows the list of registered users. The user modify sub module is designed to modify the user details. The user delete sub module is proposed to remove the selected user from the registered user list. The authorized users sub module is designed to show the active users that are connected with the grid authentication server. The user id, user name, IP address, home agent and foreign agent details are displayed in the authorized users list form.The terminal proxy module is designed with two sub modules. They are terminal proxy list and terminal proxy details. The terminal proxy list shows the list of terminal proxy applications. The terminal proxy name, IP address and node count details are listed in the terminal proxy list. The terminal proxy details sub module is designed to show the list of nodes under the selected terminal proxy. The authentication module is designed with three sub modules. They are authentication request, update log and log view. The authentication request sub module handles the authentication request that are received from the terminal proxy during the initial connectivity operations. The authentication request form shows the terminal operator name, terminal proxy name, request and requested time details. The update log sub module is designed to maintain the log files for the terminal operators. The log maintains the mobility information for each terminal operator. The log view sub module is designed to show the log data.

C. *Terminal Proxy*

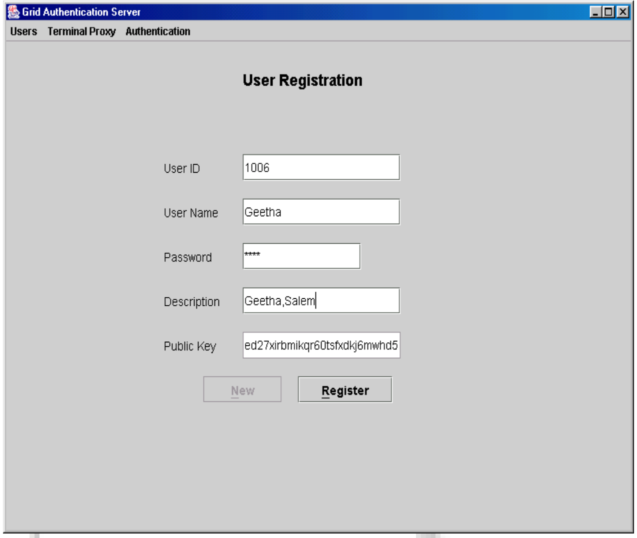
The terminal proxy application is the intermediate application between the grid authentication server and the terminal operator application. The terminal proxy application is loaded in a machine under each coverage area. All the terminal operator applications are connected with the grid authentication server via the terminal proxy application. The terminal operator authentication is done under the terminal proxy environment. The authentication operation is invoked in two instances. They are terminal operator initialization and terminal operator mobility situations. The initial authentication is done with the user id, password and key value for the users. The mobility authentication is done with the user id, password, session key values. The mobility authentication also uses the time stamp for the authentication. The one way hash function and Advanced Encryption Standard (AES) algorithm are used in the authentication process.

The terminal proxy application is divided into two major modules. They are terminal operators and session key management. The terminal operators module is designed to manage the terminal operator authentication process. This module is divided into two sub modules. They are connected node and visited nodes. The connected nodes sub module is designed to list out the nodes that are connected under the terminal proxy environment. The initial authentication is performed during the node connectivity The visited nodes sub module is designed to show the node mobility under the terminal proxy environment. The visited nodes sub module lists the user id, user name, home agent and foreign agent details with visited time .The session key management module is designed with two sub modules session key repository and session key distribution. The session key is used to secure the visited notes authentication details. The system maintains a collection of session keys under the session key repository.The session keys are displayed with session key value and generated time details. The system uses 128 bits sized session key. The session key distribute module is designed to distribute the session key for the terminal operators. The session keys are used for the current session only. Each session the system uses a new session key value. The used session key values are removed from the session key repository.

D. *Terminal Operator*

The terminal operator application is the bottom level application. All the grid nodes are refered as terminal operators. The resource sharing and resource allocation tasks are carried out under the terminal operator environment. The terminal operators has the facility to move across the grid environment. The terminal operators are monitored by the terminal proxy under their coverage area. The authentication server is used to authorize the terminal operator through the terminal proxy applications. The terminal operators are authenticated in two ways. They are initial authentication at the place of home agent and the authentication at the foreign agent environment during the visiting process. The terminal operator application is divided into four sub modules. They are terminal proxy list, mobility process, mobility report and log view. The login form is used to connect the terminal proxy with the grid authentication server. The user id, password and terminal proxy address are used in the login form. The terminal proxy list shows the list of available terminal proxy under the grid server environment. The terminal proxy authenticates the terminal operator with the help of the grid authentication server.

The mobility operation sub module is designed to perform terminal operator movement under the terminal proxy environment. The terminal operators moved and authenticated with the foreign agents. The time stamping and Advanced Encryption Standard (AES) algorithms are used for the terminal operator authentication process. The one way hash function is also used for the terminal operator authentication process. The mobility report shows the nodes mobility details. The log view sub module is designed to show the authentication request and their results under the grid authentication server application. The log view shows the user id, user name, IP address, terminal proxy name, foreign agent, log message and updated time details. Fig illustrates the modules of grid authentication.



User Registration

User ID: 1006

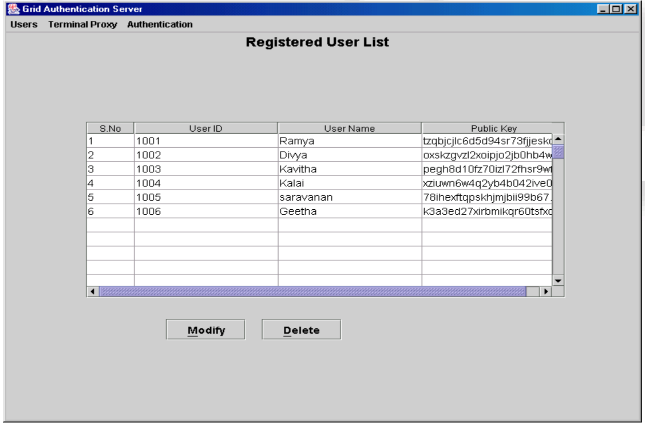
User Name: Geetha

Password: ****

Description: Geetha,Salem

Public Key: ed27xirbmikqr60tsfxdkj6mwhd5

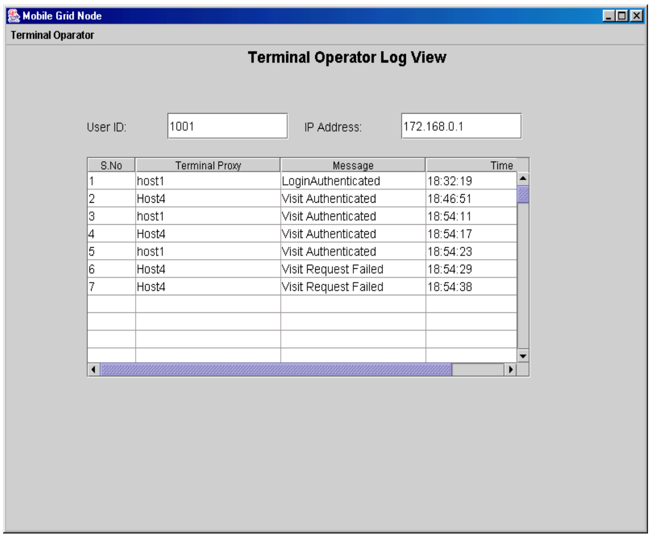
Fig. 3:



Registered User List

S.No	User ID	User Name	Public Key
1	1001	Ramya	tzqbjcjlc6d5d94sr73fjjeskc
2	1002	Divya	oxskzgvzl2xoipjo2jb0hb4w
3	1003	Kavitha	pegh8d10fz70izl72fhsr9wt
4	1004	Kalai	xziuwn6w4q2yb4b042ive0
5	1005	saravanan	78ihexftqpskhjmjbii99b67.
6	1006	Geetha	k3a3ed27xirbmikqr60tsfxc

Fig. 4:



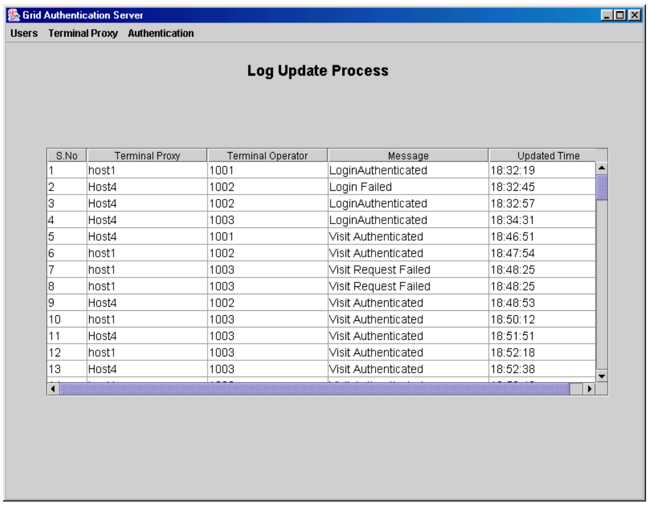
Terminal Operator Log View

User ID: 1001

IP Address: 172.168.0.1

S.No	Terminal Proxy	Message	Time
1	host1	LoginAuthenticated	18:32:19
2	Host4	Visit Authenticated	18:46:51
3	host1	Visit Authenticated	18:54:11
4	Host4	Visit Authenticated	18:54:17
5	host1	Visit Authenticated	18:54:23
6	Host4	Visit Request Failed	18:54:29
7	Host4	Visit Request Failed	18:54:38

Fig. 5:



Log Update Process

S.No	Terminal Proxy	Terminal Operator	Message	Updated Time
1	host1	1001	LoginAuthenticated	18:32:19
2	Host4	1002	Login Failed	18:32:45
3	Host4	1002	LoginAuthenticated	18:32:57
4	Host4	1003	LoginAuthenticated	18:34:31
5	Host4	1001	Visit Authenticated	18:46:51
6	host1	1002	Visit Authenticated	18:47:54
7	host1	1003	Visit Request Failed	18:48:25
8	host1	1003	Visit Request Failed	18:48:25
9	Host4	1002	Visit Authenticated	18:48:53
10	host1	1003	Visit Authenticated	18:50:12
11	Host4	1003	Visit Authenticated	18:51:51
12	host1	1003	Visit Authenticated	18:52:18
13	Host4	1003	Visit Authenticated	18:52:38

Fig. 6:

IV. CONCLUSION

The grid environment is used to share hardware and software resources. The wireless grid environment is constructed with wired and wireless nodes to share their resources. The security is the important factor in all grid environments because the nodes are connected from different network environment. The user authentication is the key security issues under the mobile grid environment. The system is implemented to provide dynamic authentication mechanism for mobile grid nodes with one way hash function, time stamp and Advanced Encryption Standard algorithm techniques. The authentication process is dynamically performed for home network and visited network access. The system is implemented as three major applications grid server, terminal proxy and grid node. The users are connected with the grid server using the grid node application. The grid server authenticates the grid nodes with the support of termianl proxy application. The initial authentication is carried out under the home network and the visited node authentication is carried out under the foreign agent environment. The system is tested with different terminal proxy and node environment. The node mobility process is also tested with different node movement operations. The authentication process is done with dynamic encryption mechanism with one way hash function and time stamp techniques. The Advanced Encryption Standard (AES) algorithm is used secure the authentication process. The system is a feasible solution for dynamic user authentication under cross platform environment.

REFERENCES

[1] L Pearlman, et al., “A Community Authorisation Service for Group Collaboration”, in Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks. 2006 IEEE.

[2] F. Azzedin and M. Maheswaran, “A Trust Brokering System and Its Application to Resource Management in Public Resource Grids”,inProceedingsofIPDPS2004.

[3] Ronghui Wu , Renfa Li , Fei Yu “Research on User Authentication for Grid Computing Security”IEEE 2008

[4] Brajesh Goyal,Shilpa Lawande, “Grid Revolution: An Introduction to Enterprise Grid Computing”, Publisher: McGraw-Hill Osborne Media; 1st edition,2009.

[5] Elliotte Rusty Harold, “Java Network Programming”, O’Reilly, 2nd Edition, 2000.

[6] Foster, C Kesselman, G Tsudik, and S Tuecke, “ A Security Architecture for Computational Grids”, in Proc 5th ACM Conference on Computer and Communications1998

[7] Foster, I., Kesselman, C. and Tuecke, S., “The Anatomy of the Grid: Enabling Scalable Virtual Organizations”, International Journal of Supercomputer Applications, 2001.

[8] Fran Berman, Geoffrey Fox, and Anthony J.G. Hey, “Grid Computing: Making The Global Infrastructure a Reality”, Wiley Series in Communications Networking & Distributed Systems, 2003.

[9] Ghassan Chaddoud Isabelle Chrisment Andr´e Schaff ,LORIA – INRIA “Dynamic Group Communication Security”, Campus Scientifique - BP239 54506 Vandoeuvre-Les-Nancy – FRANCE, 2001.

[10]Howard Chivers, John A. Clark, and Susan Stepney, “Smart Devices and Software Agents; the Basic of Good Behaviour”, in Proceedings of the first International Conference on Security in Pervasive Computing 2012.