Securing And Preventing Man In Middle Attack In Grid Using Open Pretty Good Privacy (PGP)

Anuradha Anugurala
Dept. of Computer Science and Engineering
Sri Sai College of Engineering and Technology
Badhani, Punjab, India
Email: anuradhaanugurala@gmail.com

Anshu Chopra
Dept. of Computer Science and Engineering
Sri Sai College of Engineering and Technology
Badhani, Punjab, India
Email: anshuchopra19@gmail.com

***Abstract*—As we know that security is an important issue in distributed system, that create many problems when a user want to access, or accessing services through the internet then credential management acting a main role in enhancing the security of that system, or an organization. In this proposed work w provide security solution with the help of Open PGP (RFC 4880) certificates in Grid Framework. Open PGP is nothing but it is an email encryption standard. In explanation I want to say that X.509 certificates are issuing by certification authority (CA) that certified by multiple companies, it secure by own point of view but when it is used distributed Grid system infrastructure then it becomes quite unsecure, when updating alert send to admin of the database through email then some email attacks may be possible like man in middle attack, pretexting, phishing etc. in this propose work we presented a framework which uses open PGP to prevents man in middle in the grid computing environment and provide robust and secure grid system.**

***Index Terms*—Grid computing, X.509, PGP, Pretexting, Man In Middle attack, security**

I. Introduction

Grid computing is a collection of computer resource that works at deferent location to achieve a same goal. To communicate between heterogeneous systems we need some standard that is called internet explosion. These standards can help to maximize interoperability, safety, repeatability, compatibility, or quality. These standards are used for resource sharing in grid computing. Resource sharing is computer resources that make availability from one host to other host on a computer network. Grid was beginnings in the mid 1990's. As we know that Grid computing is a part of Distributed computing, so lets discuss about distributed computing: In late 1970s when computer and network was linked then CPU cycle utilization concept was born. Some experiment in distributed computing that including a pair of program is called Creeper and Reaper that run on Internet's predecessor, that is ARPA network. ARPAnet is stand for advance research project agency network that is based on packet switching concept. It was funded by DARPA (Defense Advanced Research Project Agency). The grid computing was established in the year 1990s by Carl Kesselman, Ian Foster and Steve Tuecke. Thats why they known as father of Grid Computing. The idea was not to create a new network, but it is to integrate existing high bandwidth networks. So I-WAY was unified resources at multiple supercomputing centers. Actually Grid computing is an architecture of processors that combines computer resources from various domains to reach a main goal. In grid computing, the computers on the network works upon task together, thats why we can say that functioning is as a supercomputer [1]. Grid is a collection of variety of resources based on diverse software and hardware structures, computer languages, and frameworks.

The basic goal is to create the illusion of a simple yet large and powerful self-managing virtual computer out of a large collection of connected heterogeneous systems by sharing various combinations of resources. Grid computing is enabling, selection, sharing, and aggregation of distributed resources and appearing them as a single resource. Users can use resources without need to know source abstraction of the implementation from users. 'The whole is bigger than the part'. It allows users to use more resources than they independently own. Grid computing is a form of distributed computing whereby a "super and virtual computer" is composed of loosely coupled computers, cluster of network, acting in concert to perform very large task. Grid computing is a growing technology that facilitates the executions of large-scale resource intensive applications on geographically distributed computing resources [2].

A. Properties of computing Grid

- **Heterogeneity:** - Heterogeneity means collection of different resources in nature, in shape, in size, in hardware component also.
- **Scalability:** - Grid should be tolerant in handling a large number of nodes without performance reduction.
- **Adaptability:** - In a grid unwanted computational halt, software or hardware faults etc. are so high. These are the faults that handled by Resource Managers.
- **Security:** - it is well known fact that our data is so important, so data should be more secure when travelling one node to another node on the network, then much suspicious attack may be takes place when data are travelling on network. So we need trustworthy node for data transmission over the network. All the user of computer wants to be protected from malicious interventions or manipulations.

978-1-5090-3669-1/16/$31.00 ©2016 IEEE

B. consideration for Grid Security

- **Authentication:** -As we know that authentication is so important in case of identifying someone for using or providing resources in Grid system.
- **Authorization:** -In Grid system to restrict unauthorized person for using resources, Authorization concept are using.
- **Integrity:** -To prevent data tempering, we using integrity checking concept. Data tempering is nothing but it is simply data modification.
- **Privacy:** -To protect data over the network we apply some restriction by using some protocols at the time of data exchange.

this fig 1 represent layered architecture of the grid.

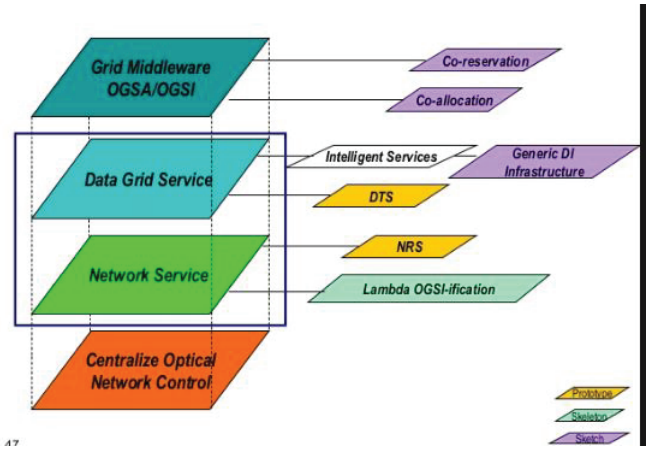

Fig. 1. layered architecture of grid computing

II. Literature Review

Network Grid Infrastructure for Industrial Sector Data, for file downloading, Grid Computational, Public Health Data Grid, Grid Infrastructure for Trading Analysis, Computational Grid for the Consulting Industry, Computational Grid Infrastructure for the Upstream Oil and Gas Industry. As we all know that data mining is a concept by which we can fetch required data from a data storage server. That stores huge amount of data in their data base. It can be called as knowledge extraction, knowledge mining from data, data archaeology, data/pattern analysis and data dredging. It is true that interest has been increasing in mining information from a huge amount of data for many purposes like scientific discoveries, business processes, and security. When we talk about security then we should keep in our mind about data security at the time of extracting from or updating to the data base in mining process. As we study about Alchemi.NET grid computing framework that were centralized in fashion that were create some problems like resource sharing from different location at a time. That was limitation of a centralized system also.

It is resolved by applying distributed system concept. Grid system applying for distributed system with some security concept at access control framework. In this they use a certificate (X.509) for authentication purpose. They also suggest a framework for future work that is ePCRN (electronic primary care research network) [3]. And this email attack may be possible, to remove that attack we can use PGP certificates (pretty good privacy) [4] that can hold multiple user signed certificates issued by CA (certification authority). By using this concept data read, write, or update alert can be get by admin directly not by email, instead of it can be get alert directly by using a web trust module. Some keywords for MINDS system like distributed data mining, security-enabled grid, access control. Actually when we talk about distributed data mining then we need to know about distributed system, means what is distributed system distributed system is nothing but it is a collection of computers that appears to user as a single system through transparency of distributed system, to enable transparency in a distributed system we need a middleware layer that behave like an interface between user and server.

As we know that to make a better grid application we have to use APIs, and to make a better interaction between client and server we have to use some useful tools. Some important key points are there that act an important role in desktop Grid. Security Barrier that is nothing but it is a connectivity of resources behind the Firewall. Actually when we use this feature then we have to know about NAT network address translator that working behind the firewall. Unobtrusiveness means there should not be any impact that affect to the running user applications. Alchemi distinguishing number of feature that comes in front when compared with some related system. That system may be SETI@HOME, XtermWeb, Entropia, GridMP, Condor etc. the comparison table can be given as:-

System / Property	Alchemi	Condor	SETI@home	Entropia	XtermWeb	Grid MP
Architecture	Hierarchical	Hierarchical	Centralized	Centralized	Centralized	Centralized
Web Services Interface for Cross-Platform Integration	Yes	No	No	No	No	Yes
Implementation Technologies	C#, Web Services, & .NET Framework	C	C++, Win32	C++, Win32	Java, Linux	C++, Win32
Multi-Clustering	Yes	Yes	No	No	No	Yes
Global Grid Brokering Mechanism	Yes (via Gridbus Broker)	Yes (via Condor-G)	No	No	No	No
Thread Programming Model	Yes	No	No	No	No	No
Level of integration of application, programming and runtime environment	Low (general purpose)	Low (general purpose)	High (single purpose, single application environment)	Low (general purpose)	Low (general purpose)	Low (general purpose)

Fig. 2. Comparison of Alchemi and some related desktop grid systems

Basically when we talk about certificate based security in grid system then public key infrastructure came in to front that acting an important role for security purpose. It is a user certificates that is provided by CA. CA is stand for certification authority. For X.509 certificate many CA are there but for OpenPGP there is only one CA present that is IEFT. User

certificate; public key certificate; certificate: the public key of a user, together with other information, rendered unfoargeable by encipherment with the private key of the certification authority which issued it.

As we know that for a valid certificate we have to satisfy the policy defined by the certification authority that will give us a certificate that proves user identity. A certification authority shall be satisfied of the identity of a user before creating a certificate for the user, Why OpenPGP is better than X.509? As we know that PGP is public key infrastructure concept that is using public key to exchanging the key. Since it is a decentralize system thats why this is better option for using in this concept. We are using OpenPGP instead of X.509 PKI, that is useful than X.509 PKI, when alert sending to user or group of user through email, then it may be possible some email attacks, by using OpenPGP concept we can resolve such problem. Because OpenPGP uses signature individually, means each user or group of user becomes a CA, while in X.509 PKI it not possible. A question may takes place here that trust level in X.509 is greater than OpenPGP and all that, but we want to say that its not correct because for such trust level problems Phil Zimmermann tells us that the certificates provided for authorization, authentication, integrity like such problems from IETF company only thats why we can see that there is multiple user to become a CA individually that may appears as trust level is decreasing but when we consider the certification company only one then the final conclusion come in front that OpenPGP is an PKI concept that is more trustworthy than X.509 PKI signature. The OpenPGP can encrypt message, email, and password. A clever attacker may use two or more than two introducer this may be a trick for attacking but it does not matter because here no chance for unsophisticated person. Because if a single company provide certificate to become a introducer then that company not become a fool because attacker cannot know about serial no and all that. So finally we can say that OpenPGP is better than X.509 PKI As we know that security is a most important factor that acting important role in grid security. And also know that mining concept that used for fetching, updating, altering, and read/write operation in huge amount of data at the data server. So we can conclude that as the time is moving further the importance of data is increasing thats why we need some secure mechanism for securing data. To secure our data at data server we should keep in mind many things that are authorization, authentication, integrity, and also updating alert when any data changes in the data base, by using network. Some attacker may be attack for fetching our important data. We need some improved version of security mechanism that can protect our data at the server when we performed transaction. So security importance will be increases day by day as attacker quality increasing day by day. So its having future scope also for a job purpose. We did try to increase the security in Grid system; here we are replacing X.509 PKI with OpenPGP PKI. They did use X.509 in the access control framework, that is strong in security point of view, but one problem may takes place that is e-mail attack possible in alert system when they sent alert about data updating to the data admin. So here some other security mechanism can apply instead of X.509 certificates that is issued by third party CA (certification authority) like Object Oriented concept can be apply for monitoring suspicious activity in Grid system, Open PGP concept that is stand for Open Pretty Good Privacy, that is designed by Phil Zimmermann. So we can use many techniques in this Grid system in distributed grid fashion.

Weissman et al [5]. have proposed about MINDS (Minnesota Intrusion Detection System) that were centralized in fashion that were create some problems like resource sharing from different location at a time. That is limitation of a centralized system also. It is removed by applying distributed system concept. Grid system applying for distributed system with some security concept at access control framework. In this they use a certificate (X.509) for authentication purpose. They also suggest a framework for future work that is ePCRN (electronic primary care research network). And this email attack may be possible, to remove that attack we can use PGP certificates (pretty good privacy) that can hold multiple user signed certificates issued by CA (certification authority). By using this concept data read, write, or update alert can be get by admin directly not by email, instead of it can be get alert directly by using a web trust module. Rupp et al [6]. have proposed some information about X.509 certificates VS. PGP certificates then we got X.509 can hold only one signed certificates, while PGP can hold multiple signed certificates. Naming scheme used in X.509; according to section 11.2 of X.509v3 Certificates associated with public key and unique distinguished name of the user it described. According to section 7 of X.509v3. Authentication relies on each user possessing a unique distinguished name. Validation procedures; as we know that for a valid certificate we have to satisfy the policy defined by the certification authority that will give us a certificate that proves user identity. A certification authority shall be satisfied of the identity of a user before creating a certificate for the user. The main goal of this proposed is to analyses the difference between both PKI. And they getting final conclusion that PGP are better than X.509 PKI. In centralized system X.509 is better than the PGP, but when they talk about in distributed organization then PGP PKI is better than X.509. YAN Fei et al [7]. have proposed the current scenario is not satisfying the Grid security for long time due distrbuted concept are used in Grid infrastructure. In this have proposed tamper resistance technique by name TC enabled GSI (Grid security infrastructure). To protect from tampring of data on server they use TPM that is stand for Trusted Protection Module. In this scenario they proposed that, a person who purchased the key, only that person can encrypt or decrypt in the TPM. Manish et al [8]. have proposed in their invited paper that there are many steps that is required in the field of analysing and modeling, the characteristics of programming model and grid syatems. Have proposed that the designed module should provide expected results as designer expect by that module; it will possible only, when each module of the model is working properly, for which they designed

in that module. And also programming should be correct in perticular module, and competible with that infrastructure also. Have proposed definition of Virtual Organization. Actually VOis a tuple (O, RS, I, PY, PL) where O is set of concrete organizations; RS is set of resource and services; I is interface by which accessing the RS; PY is stand for policy for operation of VO; PL it is set of protocol for PY; SR is standfor sequencing rules that maintain ordering and composition. Furthermore have proposed definition of Programming Model, PM is a tuple(E, OP, MC, am) where E is set of entity; OP is a set of operations; MC model of computation that consist of three model CR, COORD, COMM here CR is composition model, COORD is coordination model, and COMM is communication model. In addition to this that am is stand for abstract machine. Have proposed functions of distributed system that invited paper. Finally have proposed the modelling and charactrizing the grid scenario is future scopic.

III. Proposed Work

As we know that security is an important issue in distributed system, that create many problems when a user want to access, or accessing services through the internet then credential management acting a main role in enhancing the security of that system, or an organization.

A. Problem Formulation

As we know that when we talking about security of data then it approximately dependent on credential management. That is basically based on type of attack that is possible on the existing scenario. In MINDS system for authentication they were using X.509 PKI as a proxy certificate. There were possible brute-force attack, man in middle attack, email-attack, etc. here MINDS is stand for Minnesota intrusion detection system. We are taking some concept of security mechanism. And we are improving that short coming in a new grid scenario.

In Alchemi.NET they were using X.509 PKI certificates as a proxy certificates. The similar problems arise in that also. We can improve it by using OpenPGP PKI instead of X.509 PKI. When we talk about man in middle attack then two things strikes our mind one is issues in identity and other one is issues with integrity. Furthermore identity issue means authenticity problems, while integrity issue means, to check modification or alternation in upcoming data from server. Alternation in data is possible when private key exchange in unsecure manner, to avoid this type of problems, we have to avoid communications on WAN networks. The following scenario come in to front, if there are two parties communicating then private key should exchange on the basis of following method: -

1) Alice chooses x, calculates R1= gx mod p, and send R1 to Bob.
2) Eve, the intruder, intercept R1. She chooses Z, calculates R2 = gz mod p, and send R2 to both Alice and Bob.
3) Bob chooses y, calculate R3 = gy mod p, and send R3 to Alice, R3 is intercepted by Eve and never reaches Alice.
4) Alice and Eve calculate K1 = gxz mod p which become a shared key between Alice and Eve, however think that it is key shared between Bob and herself.
5) Eve and Bob calculate K2 = gxz mod p, which becomes a shared key between Bob and Eve, Bob however thinks that it is a key shared between Alice and himself.

B. Methodology and Objectives

To provide better security than X.509 certificates by using Open PGP (RFC 4880) certificates in Grid Framework. Open PGP is nothing but it is an email encryption standard. In explanation I want to say that X.509 certificates are issuing by certification authority (CA) that certified by multiple companies, it secure by own point of view but when it is used distributed Grid system infrastructure then it becomes quite unsecure, when updating alert send to admin of the database through email then some email attacks may be possible like man in middle attack, pretexting, phishing etc. it can be resolved when we using open PGP that is certified by only one company that is IETF (internet engineering task force). As we know that PGP can hold multiple signed certificates so may be a chance for web trust decrement but due to single company certification, trust will be increase.

My second goal is to provide better performance than previous scenario. And due to in web trust module all nodes are connected so updating alert will be automatically received by every node in Grid system, so our second goal is to provide better performance than previous scenario by using some trust mechanism like some conditions we will provide as policy that will check what type of security required for this person and what type encryption is required. It will be possible when we use a monitoring module. My third goal is to provide low cost for purchasing certificates, from CA. actually when we use OpenPGP then it will be free for licensing any certificates, that is using in email encrypting, key distributing, signature also can encrypted by this protocol. which leads to following output.

- Security of Grid system is increased
- Cost is decreased (since OpenPGP certificates are available free of cost in the IETF company for individual user with random generated key)
- The performance of used algorithm is better than X.509 PKI
- The chance of Man-in-middle attack decrease.

IV. Conclusion and Future work

In the proposed work we uses open PGP to enhance the security of the distributed grid environment. Grid is the collection of the heterogeneous resources from the different administrative domains which are dispersed geographically different location, due to the multiple administrative domains; security is the key issue to secure the grid. In this we uses open PGP to provide security which provides better security than other existing algorithm because it reduce the chance of man-in-middle attack between two parties who communicating to each other through data transmission. It is well known fact

that man-in-middle attacks takes place due lack of security for example integrity issues and identity issues. Ultimately we can say that our proposed work reduces the chance of such attacks. And also it reduces the cost of the security, since OpenPGP certificates are free available in the market.

When we talk about future work then one thing strikes our mind is that the proposed scenario can be used in ePCRN (electronic primary care research networks) and also in Alchemi.net.

REFERENCES

[1] I. Foster and C. Kesselman, *The Grid 2: Blueprint for a new computing infrastructure*. Elsevier, 2003.

[2] F. Berman, G. Fox, and A. J. Hey, *Grid computing: making the global infrastructure a reality*. John Wiley and sons, 2003, vol. 2.

[3] S. Kim, J. Kim, and J. B. Weissman, "A security-enabled grid system for minds distributed data mining," *Journal of Grid Computing*, vol. 12, no. 3, pp. 521–542, 2014.

[4] T. Banks, "Web services resource framework (wsrf)–primer v1. 2," *OASIS committee draft*, 2006.

[5] S. Kim, J. Kim, and J. B. Weissman, "A security-enabled grid system for minds distributed data mining," *Journal of Grid Computing*, vol. 12, no. 3, pp. 521–542, 2014.

[6] N. Prohic, "Public key infrastructures–pgp vs. x. 509," in *INFOTECH Seminar Advanced Communication Services (ACS)*, 2005, p. 58.

[7] Y. Fei, Z. Huanguo, S. Qi, S. Zhidong, Z. Liqiang, and Q. Weizhong, "An improved grid security infrastructure by trusted computing," *Wuhan University Journal of Natural Sciences*, vol. 11, no. 6, pp. 1805–1808, 2006.

[8] M. Parashar and J. C. Browne, "Conceptual and implementation models for the grid," *Proceedings of the IEEE*, vol. 93, no. 3, pp. 653–668, 2005.