

# The development of Grid computing with the Encryption techniques and Public Key Infrastructure (PKI)

G.Lakshmi Preya<sup>1</sup> M.Narayanan<sup>2</sup>

<sup>1</sup>UG Scholar <sup>2</sup>Assistant Professor

<sup>1,2</sup>Department of computer science engineering

<sup>1,2</sup>Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, Tamil Nadu

**Abstract**— Grid computing is considered as a special request for dealing out the data storage space of several number of computers. Secure logging, key management, allocation and credential life span and renewal is needed for better performance in the grid based systems. Parallel type of processing is also done in Grid computing system. Grid Security Infrastructure (GSI) gives Globus Toolkit and also Public Key Infrastructure (PKI) is considered to be the proposed work. Encryption techniques namely Symmetric encryption, asymmetric encryption are proposed for providing best security and develop the performance to the highest level. Symmetric encryption, asymmetric encryption encrypts and decrypts the message in the successful way. This concept is proposed for the grid security.

**Key words:** GSI, PKI, Symmetric encryption, asymmetric encryption, grid computing.

## I. INTRODUCTION

Many computers are used all over the world by different people. Though "the Grid" is considered as a dream and the "grid computing" is previously actuality. If we connect many computers a single, huge called then it is called as super-powerful computer. This single, simple and huge, global computer is made up so of grid . The grid is a framework or a structure of spaced blocks which are attached corresponding or cross to each other. Grid computing is purely considered as a group of computer assets which are gathered together from various remote places. This from a single network or a system and produce a virtual supercomputer through linking the additional power of all the computers on the grid. Grid computing structures work on the opinion and the standards of the mutually shared assets. Grid size differs with some relevant quantity.



Fig.1: Grid computing

Grid computing is shown in the fig.1 which is used to share, collect hosts, does services all over the world and grid is considered as a important thing in the modern world. A grid computing system runs on the same operating system or it can also be performed in the basis of inter-networked systems and also it access the local machine's assets. It basically includes large numbers of data and files. Finally it provides high performance systems.

Faces of Grid Computing

- Shared computing
- Clustered computing
- Utility computing,
- Cloud computing

The grid computing system uses the same idea of the other computing. It generally shares the resources with many computers all over the world to finish the workload very easily and effectively. The computer assets are considered to be the following:

- Central Processing Unit
- Memory
- Storage

## II. UNIQUE QUALITY OF GRID COMPUTING SYSTEM

The majority of the common techniques motivate software or the hardware engineers to look after the data by encrypting it. The need of encrypting the data is only for encoding it so that it will be decoded by the correct person for using the data and we can access it safely. This is why the hacker creates his own a grid system for cracking the encrypted data. This is done because the encrypting the data uses advanced and complicated methods to encode the data. This is why the hackers goes for a grid system. Because it takes years to crack the encrypted data with the help of the normal computer. The powerful grid computing system shrink the moment of time to decode the encrypted data.

## III. RELATED WORK

In this paper, huge profit is produced by the cross-fertilization is given by the resources of the distributed computing research community. Information provided is both fixed and active in nature and it can be recovered from anywhere. Data duplication (i.e. replication) technique utilized in this paper to many distributed storage space arrangement for humanizing the performance and ease of use to the greater extent. Grid eventually provides large existing raised area in the validation of best outcome [1].

To productively face the interoperability like web services, improving the performance etc is the major aim of this paper . OGSA architecture is used to develop the interoperability from time to time. Grid Testbed provides good scientific (i.e. hi-tech) and political architecture. To

produce a secured message can be sent through the transport protocol which is the required technique. The additional aspect which it can make use of Globus Toolkit, Grid Security Infrastructure, profitable productions and security [2].

Here the grid obtains large calculation and also the optimize the exploitation of assets with the help of composite algorithms which are being developed. So consider that the grid computing all the way through is committed with the fibre optic links [3].

In this paper, Security structural design is intended for large-scale scattered calculation. this architecture gives a rigid establishment for the analysis of many number of complicated mechanisms. proxy tackles the particular sign-on requirement easily. This stay away as of the be in touch with user credentials. encryption is not used inside the connected protocols, export control issues, international use are easily completed. allocation mechanisms used to hold up the scalability to the huge numbers of assets and also the users [4].

The main aim of this paper is to provide additional wide-ranging investigation in the security which is provided in grid computing. Many solutions are given both in technical way and also in the non-technical point of view. In this paper, security supplies best validation key, permit limited access managing mechanisms, Protect the credentials in the right way, Interoperability, Exportability and it basically hold up used for executing the outcome for various solutions [5].

Computational Grids executes latest science and also build up the latest applications. Grid protection must go beyond the offered techniques. Several ways are provided to contact the assets of a Computational Grid in the best way. exclusive security requirements is needed for grid and the suggestion must be given mutually to the resource client as well as to the resource contributor. The extensive aim of this situation is in the direction of increasing the alertness and the responsibility of security problem in the Grid Computing [6].

Grid computing have the preference to be the platform for the upcoming generation in the e-Science experiments. Grid computing can be progressed away from the scientific purpose and also into the ordinary IT communications. Globus toolkit permit users to access the resources which are even in isolated or distant areas. This provides verification, the data is encrypted and mainly the center of attention is the grid service. Gridbus focus on user-level Grid services and also manage the grid assets [7].

The traditional power systems basically increases the competence, dependability, and completely it decreases the costs in the grid systems. In this paper, the proposed works are implicit deny policy, vulnerability resources creates a heterogeneous network., Virtual Private Network (VPN). Grid is used for Controlling the system and also providing security. Here Information and Communication Technologies (ICT) is absolutely used in grid systems. Through this paper, the best security solutions are provided for the smart grid technology [8].

In this paper, PKI and trusted computing techniques are used very powerfully and it completes the security architecture in the best way. Certificate lifecycle

managing equipments, trust based fasten security, etc are achieved. National Institute of Standards and Technology is used for better improvement in the grid technology and also for completing the initial steps rapidly. The security technology designed for the smart grid system is extremely distended [9].

Grid is considered for Information Technology (IT) communications in the upcoming period. It assure towards the IT world to alter and convert calculation, announcement, and teamwork together. This technology provides a outcome as extensive range of network-delivered services as over the grid computing system. Here, it shows good enlargement in the performance basis and also operation. Separate web services will be provided to improve the scalability of grid [10].

#### IV. SECURITY ISSUES

Security requires three basic things. They are verification, approval, and encryption. The other security requirements are access control, data integrity, privacy, Secure logging, key management, allocation and credential life span and renewal etc. A grid resource should be verified previously to the checks that can be completed when the required access or process is permitted inside the grid. The Grid Security Infrastructure (GSI) offers a Globus Toolkit and also Public Key Infrastructure (PKI) so that it can present a technical outline or a frame.

#### V. PROPOSED WORK

- In this paper our main aim is to provide good security for the grid. so we proposed 3 things in this paper.
- They are Symmetric encryption, Asymmetric encryption and Public Key Infrastructure (PKI).

##### A. Symmetric encryption:

In the symmetric encryption, the similar secret key is used for both encrypting and decrypting the data. This is done to make sure whether the data is read only by the two kinds of people (i.e.) sender and receiver. The sender encode the data with encryption technique and receiver decodes the data with decryption technique with the help of one shared secret key. Encryption is done with the plaintext and the decryption is done with the cipher text.

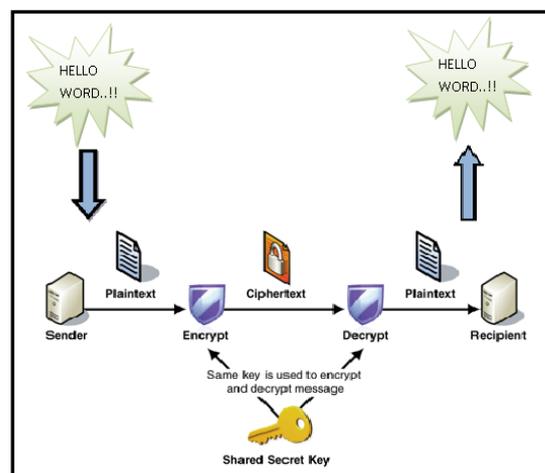


Fig. 2: Symmetric key encryption

Figure 2: shows the Symmetric key encryption using one shared secret key (i.e. same key) . This can improve the security issues in the field of grid computing.

**B. Asymmetric encryption:**

Asymmetric encryption involves in additional processing assets than we see in symmetric encryption technique. That is why asymmetric encryption is frequently make the best by adding up once to encrypt the message which we sending and also encrypting the shared key asymmetrically. This technique decreases the original size of the data which is asymmetrically encrypted in the process and this develops the overall performance of the grid in the basis of security. consider an example, the bank (any bank name) bring out a network service to offer the business clients among the capacity to upload the payroll bank account relocation. But direct deposit bank account information is believed as a sensitive approach in favor of both the business and the client. By cooperating to this type of problem, the information can end in the use of illegal account actions. For this reason, the bank needs communication including the bank account data which are already encrypted as they exceed in among the clients and the network service to give data privacy.

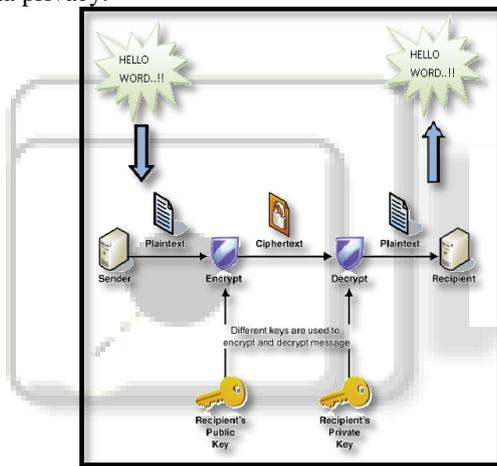


Fig. 3: Asymmetric encryption

Figure 3: shows the asymmetric encryption, were the different keys are used for encrypting and decrypting the message which has sent by the sender to the receiver.

**C. Public Key Infrastructure (PKI):**

Public Key Infrastructure (PKI) is a type of an arrangement that is used to connect the public keys by way of the personal or particular user which can be identified by the resources of a Certificate Authority (CA). This CA professionally Issues, removes, and also archive the certificates. In some kind of Public Key Infrastructure (PKI) environments, a Registrant Authority (RA) work along with the Certificate Authority (CA) to make the job easy. The validation authority (VA) can give this information instead of Certificate Authority.

figure 4: shown the public verification of the public key information with the help of Public Key Infrastructure. Certificate Authority (CA) is used to offering the requirements. These are the security concepts to increase the protection in grid computing technique.

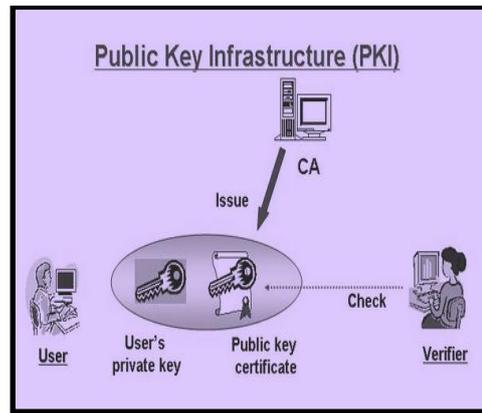


Fig. 4: Public Key Infrastructure (PKI)

**VI. CONCLUSION**

Grid Computing is the super-powerful computer. This name is achieved by the extreme performance of the grid. Symmetric encryption, Asymmetric encryption and Public Key Infrastructure (PKI) are proposed in this paper and we got the best security using these techniques. Grid not only provides good security with the help of these techniques but also it provides high performance in authentication, data and message integrity process. Though the implementing cost is low for grid it provides best outcome in improving the speed of the systems than the normal computers does. This improves scalability to use grid computing system for large numbers of resources and also the users.

**ACKNOWLEDGEMENT**

I hereby like to communicate my special thanks and gratefulness to my guide Mr. M.Narayanan who is perusing as assistant Professor in Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha University, Thandalam, Chennai, Tamil Nadu (India).He gave me the excellent chance to write this paper. His valuable suggestions and guidance motivated me in carrying out a thorough investigation. I learnt several concepts and techniques which enhanced my knowledge also.

**A. Facts about Grid:**

- The dreams of the grid computing system (which comprises of distributed computing, Web services object-oriented programming etc ) were brought collectively by the 3 legends Ian Foster, Carl Kesselman, and Steve Tuecke, broadly they were called and considered as the "fathers of the grid".
- GARUDA, India's first national grid initiative conveyed collectively in the field of academic, scientific and research communities intended for increasing the data and also it have to calculate the concentrated request through the assured Quality of Service (QoS). This finished on March 2008, skilled its deliverables through linking 17 capitals transversely and it is still organizing the grid computing request in the sufficient manner.
- ORACLE uses Grid technology. Oracle software is particularly planned for grid computing, for conveying a superior quality of service for the business oriented development at a very less cost.

Grid version of oracle is considered as one of the best version.

#### REFERENCE

- [1] Henri Casanova, "Distributed Computing Research Issues in Grid Computing", NACM SIGACT News, Volume 33 Issue 3, September 2002 ISSN: 0163-5700.
- [2] Jianmin Zhu et-al, "Secure Grid Computing", Technical Report UTDCS-64-06, Department of Computer Science. The University of Texas at Dallas. December 2006.
- [3] Poonam Dabas Anoop Arya, "International Journal of Advanced Research in Computer Science and Software Engineering", Volume 3, Issue 3, March 2013 ISSN: 2277 128X.
- [4] Ian Foster et-al, " A Security Architecture for Computational Grids", ACM New York, NY, USA ISBN: 1-58113-007-4.
- [5] Zohre Zare, "Security in grid computing", 5<sup>th</sup> SASTech 2011, Khavaran Higher education Institute, Mashhad, Iran. May 12-14.
- [6] Marty Humphrey, Mary R. Thompson, "Security Implications of Typical Grid Computing Usage Scenarios", ISSN 1082-8907, DOI:10.1109/HPDC.2001.945180.
- [7] Rajkumar Buyya and Srikumar Venugopal, "A Gentle Introduction to Grid Computing and Technologies", Computer Society of India.
- [8] Fadi Aloul, et-al, "Smart Grid Security: Threats, Vulnerabilities and Solutions", International Journal of Smart Grid and Clean Energy, volume 1, no.1, September 2012.
- [9] Anthony R. Metke and Randy L. Ekl, " Security Technology for Smart Grid Networks", IEEE Transactions On Smart Grid, Volum.1, No. 1, June 2010.
- [10] [www.witsa.org](http://www.witsa.org)