# Dynamically Changing the Symmetric Encryption Algorithm for Improving Security and Performance during Data Transfer in Grid Networks

N.Thenmozhi
Department of Computer Science
N.K.R. Govt. Arts College
Namakkal, India

M. Madheswaran
Department of ECE
Muthayammal Engineering College
Rasipuram, India

## ABSTRACT

In grid design authentication, authorization and confidentiality of the communication between computers are important security requirements. Without the functionality, the integrity and confidentiality of the data processed, the grid would be at risk. There are many different tools and technologies, which are available to ensure secured grid environment. The symmetric and asymmetric encryption algorithms are commonly used algorithms in grid software to provide necessary security, even though symmetric encryption algorithm significantly will affect the network communication performance.

The previous work relied on the use of encryption and decryption at the application layer has an impact on the application layer performance and in the network layer performance. In the proposed work, instead of using a single encryption algorithm different encryption algorithms were selected arbitrarily during processing of each packet. The performance has been measured through simulation studies on NS2 by simulating these algorithms on GARUDA Grid Network Topology.

## Keywords

NS2, Encryption, GridFTP, PPLive, ERNET, GARUDA.

## 1. INTRODUCTION

Grid computing suggests a computing paradigm similar to an electric power grid in which a variety of resources contribute power into a shared pool for many consumers to access as on a needed basis. In such a big environment, security issues are serious concern to transfer volume of data. To provide necessary security, symmetric and asymmetric encryption algorithms are commonly used algorithms in grid software. Encryption is the process of encoding plaintext into cipher text and decryption is the reverse process [7, 8].

Symmetric encryption classified into block ciphers and stream ciphers. Block cipher is a symmetric cipher, which encrypts a message by breaking it down into blocks (commonly of 64 bits) and encrypting data in each block. A block cipher encrypts the text in fixed sized blocks. Block ciphers take a number of bits, encrypt them as a single unit, and operate on blocks of bits at a time. Some examples of block ciphers are Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES), Blow Fish, Rivest Cipher (RC2), RC5, RC6, IDEA and Twofish [1].

There are several simulators and tools such as Bricks, ChicSim, GrenchMark, GridNet, GridSim, JFreeSim, MicroGrid, NSGrid, OptorSim and SimGrid for studying various aspects of a grid network like resource allocation, management and task scheduling [9]. For performance analysis in MANETs, commonly used network simulators include NS2, GloMoSim, QualNet and OPNET. Most of the existing grid network simulators and tools are having lack of support for simulating encrypted data transfer and some of the network layer aspect of grid simulation. The results of this research will try to fulfill these missing aspects of a grid network simulator. Further, it will propose a new model for enhanced performance.

The Europe-China Grid Inter Networking (EC-GIN) project [9] provides some preliminary traffic models for studying the network aspects of the grid simulation. By using those traffic models, this research expected to provide framework for studying secured data transfer mechanism of grid networks. GARUDA is a project, which is deployed on the existing Indian Wide Area Network architecture called Education and Research Network (ERNET). This research work can be extended to the functionality of the traffic models of EC-GIN project and apply the same on Indian grid network called GARUDA to evaluate the network communication performance.

The present research work identifies the following aspects of study and analysis to form the scope of the study. Based on the findings of the study, the work proposes random selection of symmetric encryption algorithms to provide better security and performance evaluation.

## 2. RELATED WORK

The impact of using different popular and commonly used symmetric key cryptography algorithms for encrypting data in a typical grid-computing environment was discussed in [16]. In this work, the researcher is discussing the dynamically selected different encryption algorithms over time and their impact on network layer performance.

S. Corson and J. Macker [2] have stated that the average number count can be used to measure pure algorithmic efficiency instead of bit count to transmit data. This measure tries to capture a protocol’s channel access efficiency, in high contention based link layer.

B.P. Van Leeuwen and M.D. Torgerson [3] explained cryptographic features, which have been applied to each of the message involved in the data link layer exchange. The overall network performance can be quantified based on the performance impact on the lower layer cryptographic features. End-to-end delay of application layer messages is found to increase when cryptographic features are used in MANET.

Border Gateway Protocol (BGP) conformance test tools [5] performed their tests as a dialog: they send packets to the router being tested and receive the packets sent in response, then analyze the response to determine the action to take. Kannan Srinivasan et al. [10] provided a modification for BGP and the result showed that there was decreased packet loss in the data transfer and they also analyzed how shortcomings could be rectified.

Himanshu khurana et al. [11] evaluated elliptic curve cryptography and RSA in terms of their computation and communication overheads for today’s grid systems. A high performance file transfer mechanism for grid computing to achieve excellent performance in a computational grid and used the concept of Lightweight Object-Based (LOB) file transfer System was discussed in [12].

Manghui Tu et al. [15] discussed two heuristics algorithms for achieving a good performance in reducing communication cost, which was close to optimal solutions.

The project EC-GIN (Europe-China Grid Internetworking) [9] was developed a tailored network technology in dedicated support of Grid applications. These technical solutions will be supplement with a secure and incentive-based grid services network traffic management system, which will balance the conflicting performance demand and the economic use of resources in the network and within the grid.

Education and Research Network (ERNET) was the first dedicated and integrated step towards enabling the research and education community in India. Dissemination, training and knowledge transfer in the field of computer communication and information technology are an integrating part of ERNET mission. The ERNET network has 15 Points of Presence spread throughout India serving 1389 institutions, including 152 universities, 284 agricultural universities and many other research organizations. It has 14 points of peering for Internet bandwidth connectivity using submarine cables.The network comprises a mix of terrestrial and satellite-based wide area networks. ERNET is the first network in the country to provide dual stack access of Internet protocol version 6 (IPv6) and Internet protocol version 4 (IPv4) test beds to its users to develop, test and implement IPv6 based mail, Domain name Services, Web applications and products [18, 20].

GARUDA initiative is a collaboration of science researchers and experimenters on a nation- wide grid of computational nodes, mass storage and scientific instruments that aims to provide the technological advances required to enable data and compute intensive science of the 21st century The Department of Information Technology (DIT) has funded the Center for Development of Advanced Computing (C-DAC) to deploy the nationwide computational grid 'GARUDA' which today connects 45 institutions across 17 cities in its Proof of Concept (PoC) phase with an aims to bring "Grid" networked computing to research labs and industry. In pursuit of scientific and technological excellence, GARUDA PoC has also brought together the critical mass of well established researchers. The PoC network was established at all the GARUDA partner institutes in close collaboration with ERNET who are responsible for the operation, maintenance and management of this network [18, 19, 21]. Garuda can offer the strength of data grid and power of computational grid. The applications of GARUDA are weather and climate modeling, distance education, Bio sciences, Conputational Fluid Dynamics and Students grid projects. Grid enablement of DMSAR is a RADAR based airbone earth imaging system through which the real time suituations of any natural and man induced disasters can be mapped even in rough weather conditions[19].

The researcher will use NS2 to simulate the network. Till now, there is no option for simulating security things in NS2. NS2 is an object oriented simulator, written in C++, with an OTCL interpreter as a frontend. Users create new simulator objects through the interpreter. There are two basic types of applications: traffic generators and simulated applications. Currently, there are four C++ classes derived from the traffic generator class. Traffic Generator: EXPOO_Traffic, POO_Traffic, CBR_Traffic, and Traffic Trace [9].

Here we have simulated a new encrypted traffic generator and find out the received packets, dropped packets while transfer the data, and time delay at the receiving end. Based on the EC-GIN the proposed work is modeled on the Indian grid network topology GARUDA, to study the impact of the encryption based traffic model.

In the previous work of [16], it was proved that the use of encryption and decryption at the application layer has an impact on the application layer performance as well as in the network layer performance in a typical grid computing environment. In this study, certainly this work was used to dynamically change the encryption algorithm over time to study its impact on network performance. Here, instead of using a single encryption algorithm, different encryption algorithms were selected arbitrarily during processing of each packet. The performance has been measured through simulation studies on NS2 by simulating these algorithms on GARUDA Grid Network Topology.

# 3. MODELING GRID AND GRID TRAFFIC IN NS2

## 3.1 Modeling Encrypted PPLive Traffic

Along with the rapid development of P2P file sharing and IPTV video services, P2P streaming services have become a core multi-user video sharing application on the Internet. The focus of grid technology in the video area is generally on the resource scheduling and replica management aspects, while the service traffic characteristics are still similar to the traditional video service. In depth work has already been carried out in the areas of monitoring and modeling video traffic [9]. Therefore, exploring the developing trends of grid systems, video sharing, monitoring and the analysis of P2P IPTV traffic are interesting and promising topics of research.

The time interval between two packets and the size of each packet waiting for sending out is very important when modeling actual traffic. Therefore if the model can accurately match these two characteristics, it can be said to generate traffic that is similar to the actual data. The EC-GIN project built a new traffic generator to model the actual traffic called Lognormal Traffic, which is primarily responsible for controlling the packets time interval and the packet sizes.

Our goal is to extended the traffic model of PPLive (Lognormal Traffic) to support a simulated encryption-decryption scenario. Based on traffic model of EC-GIN, an algorithm has been put forward to control the packet generation sequence. First, data initialization is performed as follows:

- Send a video packet when simulation begins.
- Compute the next video packet sending time. Put it into a variable NextT.

Next, the time needed to send the next packet is computed. To account for different packet sizes, different parameters are used to calculate inter-video packet time (variable NextT) and the inter-control packet time (array t_i). The values of t_1 to t_n are summed to variable SmallT. As long as the value of SmallT is less than NextT, t_i is used as a inter packet time for sending small packets (control packets). Otherwise, a large packet (video packet) is sent immediately with an inter-packet time of NextT - (SmallT - t_i) [9].

In addition to the above process, we have delayed the packet transmission with respect to the size of the packet to be sent and the selected encryption algorithm. So the new Scheduled Transmission Time will be equal to the sum of inter-packet time and the time taken for encrypting the packet by the selected algorithm.

In our implementation we have simulated the encryption algorithms in a typical grid network scenario just by including the encryption delay at the traffic generator using the results from [6, 13, 14]. In the traffic model of EC-GIN, they used UDP in their design. We have decided to use TCP, because, TCP is the most commonly used transport protocol in grid network communication.

To change the encryption algorithm over time, we just used random selection method. Before the event of packet transmission, an encryption algorithm has been randomly selected to encrypt the data.

## 3.2 Modeling GridFTP

In this work, we used GridFTP as a background cross traffic during evaluation of the impact of encrypted PPLive traffic. The three major parameters defined for the GridFTP simulator are Bandwidth, Parallel and Ratio [4]. In order to create the different traffic scenario files, the researcher used different types of grid traffics mentioned in EC-GIN project. They are GridFTP Traffic and PPLive Traffic. The GridFTP simulator consists of GridFTP and GridFTPSink classes. In addition, it overrides two methods for the basic Simulator class, attach-agent and connect, with which the GridFTP instance can be attached to the network node and connected to the GridFTPSink instance.

However, none of these classes match the traffic characteristics of PPLive and of GridFTP. The GridFTP tool of Globus Toolkit is one of the most important components provided by Globus for moving large amounts of data in bulk. GridFTP is based on FTP, the highly popular Internet file transfer protocol. Given the characteristics of Grid traffic often a mixture of short, sporadic service calls and bulk data transfers, a GridFTP simulation scenario differs from other traffic models and is therefore important for testing grid specific network mechanisms. The GridFTP simulator of EC-GEN was developed with the OTCL language to mimic this GridFTP traffic. The EC-GEN GridFTP is embedded in a gridftp.tcl file [9].

# 4. RESULTS AND DISCUSSION

The following NAM output (Figure 1) shows the model of GARUDA network simulated on NS2. The topology was derived from the information provided by the ERNET and GARUDA projects.

- ➢ The links shown in green are 8/34Mbps links
- ➢ The links shown in red are 2/8 Mbps links
- ➢ Nodes shown as red hexagon are backbones and POPs
- ➢ Nodes shown as blue circles are the connected institutes

In a typical grid computing scenario, the security has been generally handled at the application layer. Hence, the study was taken to simulate encryption in NS2 at application layer, with modeling a new encrypted traffic generator. A simple model of GARUDA grid network has been simulated in NS2 and the impact of different encryption schemes on network performance has been evaluated. The performance of the network with respect to different cryptography algorithms used in the application layer was analyzed by comparing time and throughput, average received packets, sent packets and end-to-end delay in different schemes over time. The Backbone and POP nodes (12 nodes) used in simulated GARUDA topology are Chennai (0), Delhi (1), Kanpur (2), Gorakhpur (3), Guwahat (4), Indore (5), Kalkota (6), Mumbai (7), Pune (8), Bhubaneshwar (9), Hydrabad (10) and Bangalore (11).

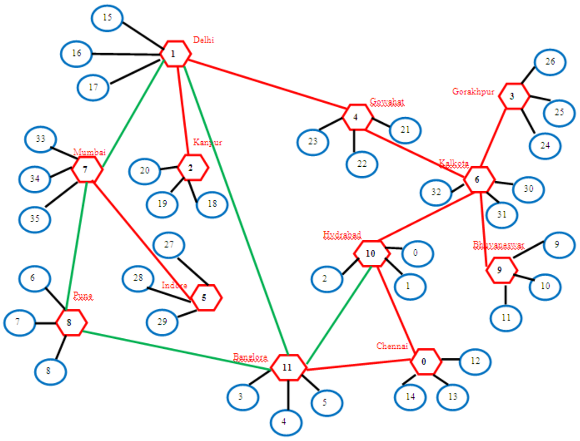

**Fig 1 : The Simulated GARUDA Topology**

The simulation parameters and their values used for this simulation are listed in the table 1.

**Table 1. Simulation Parameters**

| **Simulation Parameters** | **Parameter Values** |
|---|---|
| Number of Backbone and POP nodes | 12 |
| Number of Simulated Institution Nodes | 36 |
| Routing Protocol | DV |

| | |
|---|---|
| Backbone Link Capacity | 8/34 Mbps |
| Institution to Backbone Links | 2/8 Mbps |
| Queue Type | Drop Tail |

The experiment showed the comparison of throughput in different encryption schemes over time. The dynamic encryption scheme results showed a moderate performance than all the separate encryption schemes. The throughputs in the case of no encryption as well as the Blowfish were higher and the delay caused by the rapid use of network in these two cases was very high when comparing it with this study. The comparisons were done between average received packets, time versus average end-to-end delay packets. The variations in the arrival time of packets caused by network congestion, timing drift, or route changes in different encryption schemes were also analyzed.

Throughput is usually measured in bits per second and sometimes in data packets per second or data packets per time slot. The amount of data moved successfully from one place to another in a given period is called throughput. The comparison of throughput in different encryption schemes over time and its average are shown in the figures 2 and 3.

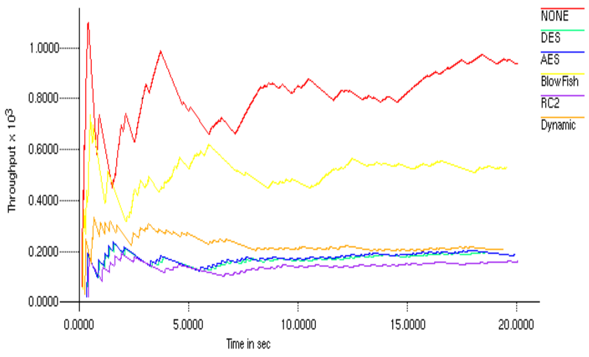

**Fig 2 : Comparison of Throughput with Time**

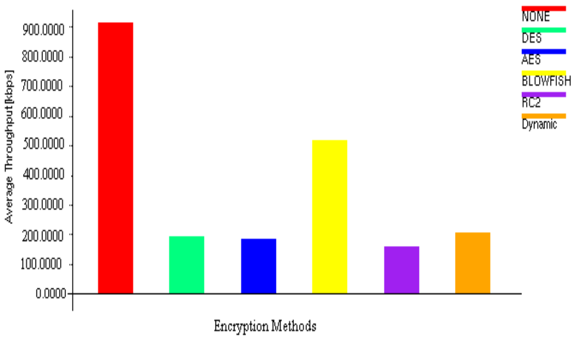

**Fig 3 : Average Throughputs for Various Encryption Algorithms**

The graph 4 shows the comparison of Average Received Packets in different encryption schemes.

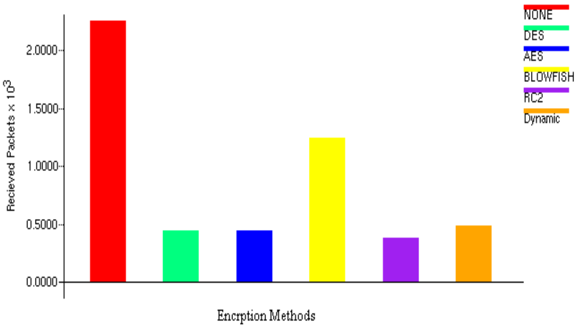

**Fig 4 : Average Received Packets for Various Encryption Algorithms**

The Figure 5 shows the comparison of end to end delay in different encryption schemes over time.

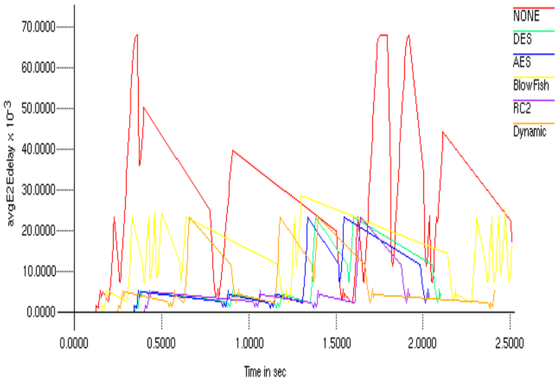

**Fig 5 : Comparison of Average End to End Delay with Time**

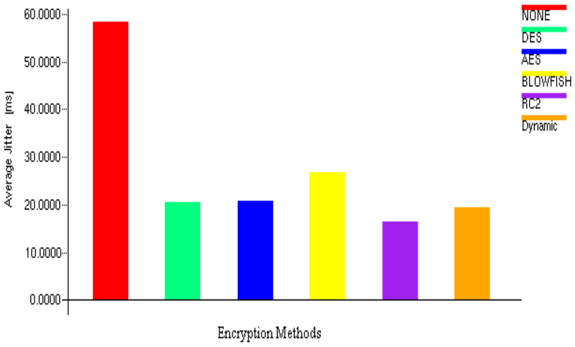

**Fig 6 : Average Jitter**

The graph 7 shows the average delay in different encryption schemes.

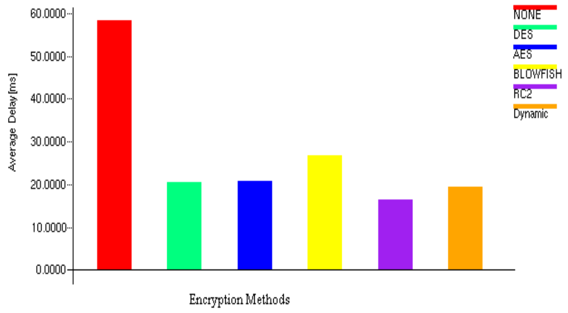

**Fig 7 : Average Delay for Various Encryption Algorithms**

The performance of the network with respect to different cryptography algorithms (DES, AES, BLOWFISH and RC2) was used in the application layer. The results analyzed and a comparison chart has been prepared, and the graph results are shown in the table 2.

**Table 2. Dynamic selection of Symmetric Encryption Algorithms Comparison**

| Results / Algorithms | Average Delay(ms) | Average Received Packets (kbps) | Average Throughput (kbps) |
|---|---|---|---|
| NONE | 58.4141 | 2259 | 915.767 |
| DES | 20.6135 | 441 | 195.211 |
| AES | 20.7513 | 450 | 185.381 |
| BLOWFISH | 26.6894 | 1242 | 517.095 |
| RC2 | 16.5053 | 387 | 158.952 |
| DYNAMIC | 19.3388 | 486 | 205.293 |

Even though all the transmitted packets were received successfully, the throughput and delay were much affected by the rapid change in queuing of the packets during the fast data transfer. This fast transmission of packet had a positive impact on throughput but a negative impact on delay. Faster the encryption algorithm higher will be the bandwidth. So it increased the delay, packet loss and drop at intermediate nodes. It has been found that the dynamic selection of encryption algorithm caused an average delay of 19.3388 msec, the average received packets are 486 kbps and the average throughput is 205.293 kbps. The randomly changing encryption algorithm during the data transfer has a positive impact on performance.

## 5. CONCLUSION

A model for grid security infrastructure has been implemented on network simulator NS2 and the impact of use of encryption algorithms in network performance has been measured. We have simulated a simplified model of GARUDA grid network in NS2 and simulated some of the basic traffic types of grid network (proposed in ECGIN). As shown in the graphs, the use of cryptography at the application layer has obvious impact on the network performance. Further, it has been shown that, randomly changing the encryption algorithm during the data transfer has a positive impact on performance. In addition to that, random change of encryption algorithm will certainly increase the effort needed to break the code by any intervening hacker and hence at least theoretically will strengthen the security. In this simulation study, we randomly changed the encryption algorithm just to study its impact on network performance.

Future work may address the issues of impact of asymmetric encryption algorithms used in a grid network for authentication and other purposes. In this work, the encryption load has been simulated on one particular traffic model. Future work may address the issues of implementing encryption on other traffic types of grid network. Also it may address the efficient ways of dynamically changing the encryption algorithm in a real communication scenario. The ways in which that change will be exchanged between communicating parties can be explored in future works. It may also address a possibility of adding QoS (Quality of Services) aspects in the process of dynamic selection of encryption algorithm.

## REFERENCES

[1] Bruce Schneier, 1996. Applied Cryptography, John Wiley & Sons, Inc , Second Edition.

[2] S.Corson and J. Macker, 1999. In the Routing Protocol Performance Issues and evaluation consideration, Naval Research Laboratory, Network Working Group, Copyright The Internet Society, MANET Performance Issues, pp.1-10.

[3] B. P. Van Leeuwen and M. D. Torgerson, 2002. Performance Impacts of Lower Layer Cryptographyic Methods in Mobile Wireless Ad Hoc Networks", SAND REPORT, SAND 2002-3340, Sandia National Laboratories, California.

[4] IBM Corporation, 2003. Introduction to Grid Computing with Globus, International Technical Support Organization.

[5] BGP - Border Gateway Protocol Conformance and Performance Testing : Sample Test Plan, 2004-XA Because Performance counts.

[6] Aamer Nadeem, A Performance Comparison of Data Encryption Algorithms, IEEE 2005.

[7] Marty Humphery, Mary R. Thomson, and Keith R.Jackson, 2005. Security for Grids, Proceeding of the IEEE, Vol 93, No.3, pp.644-650.

[8] Priya Dhawan,2005. Performance Comparison: Security Design Choices, Auerbach Publications.

[9] Europe-China Grid InterNetworking,2006. Deliverable D2.1, NS2 code for Grid network simulation, The EC-GIN Consortium, Europe-China Grid InterNetworking,

Survey of Grid Simulators, Network-level Analysis of Grid Applications, European Sixth Framework STREP FP6-2006-IST-045256.

[10] Kannan Srinivasan, Prabal Dutta, Arsalan Tavakoli, and Philip Levis, 2006. Understanding the Causes of Packet Delivery Success and Failure in Dense Wireless Sensor Networks, Technical Report SING-06-00 (//sing.stanford.edu/pub/sing-06-00.pdf).

[11] Himanshu Khurana, Radostina Koleva, Jim Basney, 2007. Performance of cryptographic protocols for High performance, High Bandwidth and High Latency Grid systems, Third IEEE International Conference on e-Science and Grid Computing 2007, pp. 431-439.

[12] Phillip M. Dickens, Illino, 2007. A High Performance File Transfer Mechanism for Grid Computing, A Technical Report Number Tr-0121, CoreGRID is a Network of Excellence funded by the European Commission the Sixth Framework Programme, Project no. 004265.

[13] D. S. Abdul. Elminaam, H. M. Abdul Kader and M. M. Hadhoud, 2009. Performance Evaluation of Symmetric Encryption Algorithms, Communications of the IBIMA, Volume 8, ISSN: 1943-7765, pp. 58-64.

[14] Diaa Salama Abd Elminaam, Hatem Mohamed Abdual Kader, and Mohiy Mohamed Hadhoud, 2010, Evaluating The Performance of Symmetric Encryption Algorithms, International Journal of Network Security, Vol.10, No.3, PP.216-222.

[15] Manghui Tu,Peng Li,I - Ling Yen, Bhavani Thurai singam, Latifur Khan, 2010. Secure Data Objects Replcation in data Grid, IEEE transaction on dependable and secure computing,Vol. 7, No.1, pp. 50-64.

[16] Thenmozhi. N, Madheswaran. M, 2010. Analysis of impact of Symmetric Encryption Algorithms in Data Security Model of Grid Networks, International Journal of Computer Science and Information Security, Vol. 8, No. 6, (September 2010).

[17] EC-GIN project, http://www.ecgin.eu/corpsite/display/dsp_Entity.asp

[18] ERNET project DOC Identifier : EU-IndiaGrid-Deliverable D3.1, 2007, http://www.eis.ernet.in/aboutus.htm, partnerlisting, Indian Network Perspectives – a article presented by Meharban Singh, ERNET India.

[19] GARUDA Project, www.garudaindia.in/html/garuda_publications.aspx, /applications.aspx, /network_fabric.aspx

[20] Europe India Grid Project, http://partners.euindiagrid.eu/deliverables/D3.1.html

[21] Subrata Chattopadhyay, CDAC knowledge part , Banglore, India, 2007, Challenges of Garuda : The national Grid Computing Initiative of India, and http://www.cdac.in/html/pdf/FINAL English Annual Report 2010-11.pdf