International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 1 | Issue – 6

Enhancing the Techniques to Secure Grid Computing

Simranjeet Kaur
Jasmer Singh Jaijee Degree College Gurne Kalan, Moonak, Punjab

ABSTRACT

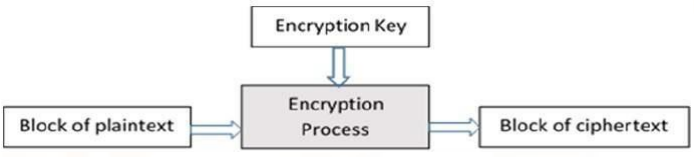
Security is important issue in every aspect in today's world if you are using the networks. Various algorithms are there to secure your network so that unauthorized user can't breach into your accounts. SO for this authentication and authorization plays an important role but apart from these use of various encryption algorithms are there for grid data security. By using these algorithms you can easily secure your network and it will also enhance the performance of our grid networks. In this paper model has been designed for grid security that is been implemented on network Simulator and the performance has been measured with the previous models. By using various cryptographic algorithms the efficiency and the packed delivery ratio is increased incredibly.

Keywords: *Encryption Algorithms, Kerberos, Authentication, Grid*

I. INTRODUCTION

The term 'grid' was comes in 1990s and grid computing is a term referring to the combination of various computer resources from multiple administrative domains to reach a common goal in advanced computer science. The term 'grid computing' suggests a network of computers in which each computer resources are shared with every other computer in the system. It is just an architecture that combines computer resources from various domains to reach a main objective. Resources like Processing power, Memory, data storage are all resources that helps the authorized users for specific task. The symmetric and asymmetric encryption algorithms are commonly used algorithms in grid software to provide necessary security. Now Encryption is a process of encoding the plain text into cipher text and decryption is the processes when you got cipher text just decode that into plain text. So decryption is just reversing that of encryption.

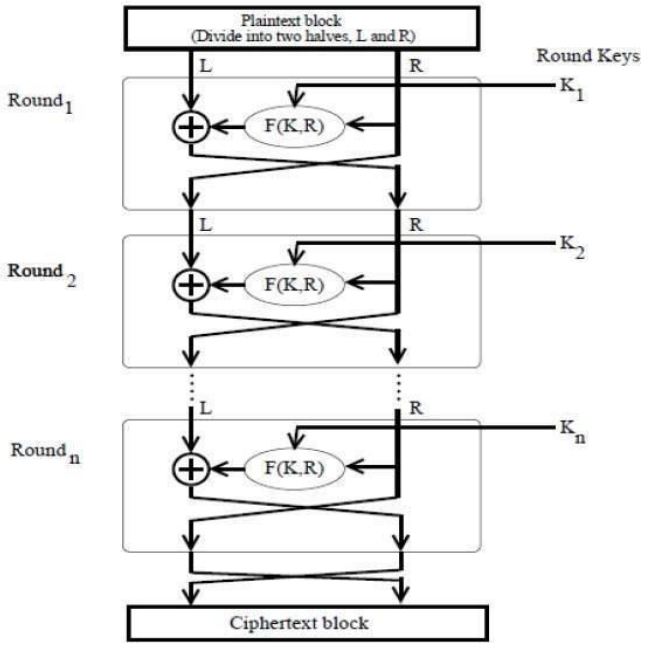
Symmetric encryption is classified into 2 categories block ciphers and stream ciphers. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher digit stream (keystream). In a stream cipher, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. A block cipher takes a block of plain text and generates cipher text generally of same size. Block cipher avoid floating values in order to minimize the energy consumption. Block cipher supports various encryption key methods.



The choice of block size does not directly affect to the strength of encryption scheme. The strength of cipher depends up on the key length. The present research work indentifies the various aspects of the enhanced traffic model for getting command on symmetric encryption algorithm those are used for security the grid. By enhancing the aspects of these algorithms various Symmetric Encryption algorithms are proposed for better throughput so that network

performance also improves and better security among the systems and obviously for the grid. The encryption process uses the Feistel structure.

Feistel Structure is shown in the following illustration −



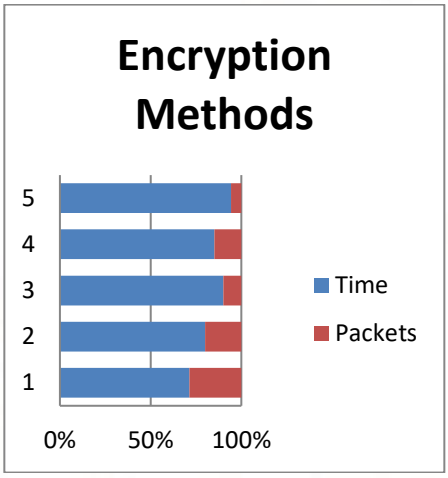
The difficult part of designing a Feistel Cipher is selection of round function 'f'. In order to be unbreakable scheme, this function needs to have several important properties that are beyond the scope of our discussion.

II. Encryption Algorithm

Security is based upon three main services: authentication, authorization, and encryption. It is needed to authenticate the grid before any requested access or operation comes in the grid. The grid user would be granted certain rights to access a grid resource, once the grid resource is authenticated within the grid. This, however, does not prevent data in transit between grid resources from being captured or altered.

However, in this work, the researcher examined its impact on total network performance. In this paper, we will study the impact of symmetric encryption algorithms in a typical grid network. The use of cryptography always help in one way or the other. Therefore, it has been decided to model an application layer encryption decryption scenario in a typical grid computing environment and study its impact on network performance through network simulations.

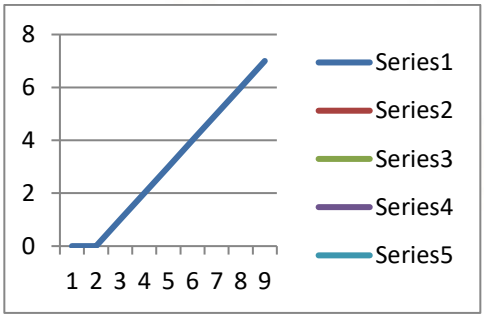
The time interval between two packets and the size of each packet waiting for being sent out is very important when modeling actual traffic. Therefore, if the model can accurately match these two characteristics, it is said to generate traffic that is similar to the actual data.



III. Security Implementation

Kerberos: Kerberos is a network authentication protocol. It is designed to provide strong authentication for client/server applications by using secret-key cryptography.

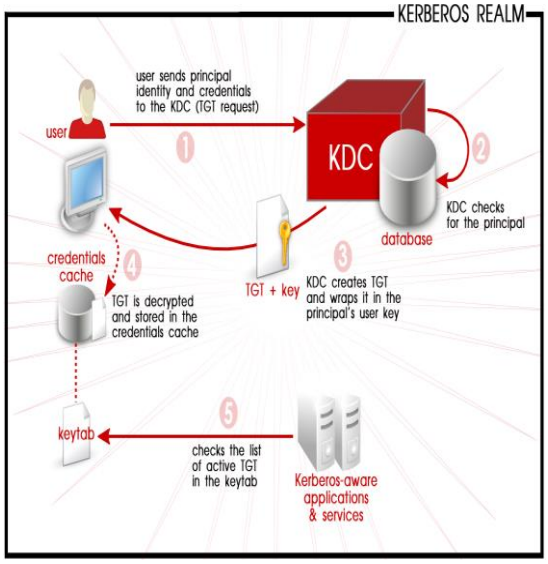
The Internet is an insecure place. Many of the protocols used in the Internet do not provide any security. Tools to "sniff" passwords off of the network are in common use by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, other client/server applications rely on the client program to be "honest" about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those which it is allowed to do, with no other enforcement by the server.



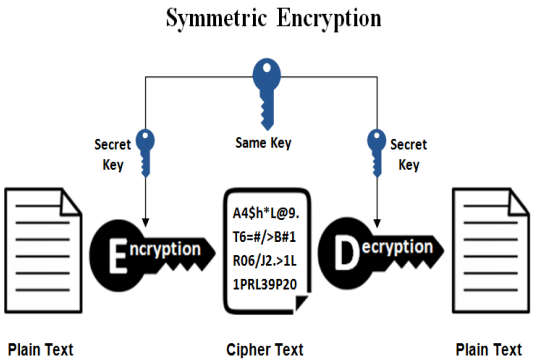
Packet vs Time

Some sites attempt to use firewalls to solve their network security problems. Unfortunately, firewalls assume that "the bad guys" are on the outside, which is often a very bad assumption. Most of the really damaging incidents of computer crime are carried out by insiders. Firewalls also have a significant disadvantage in that they restrict how your users can use the Internet. (After all, firewalls are simply a less extreme example of the dictum that there is nothing more secure than a computer which is not connected to the network --- and powered off!) In many places, these restrictions are simply unrealistic and unacceptable.

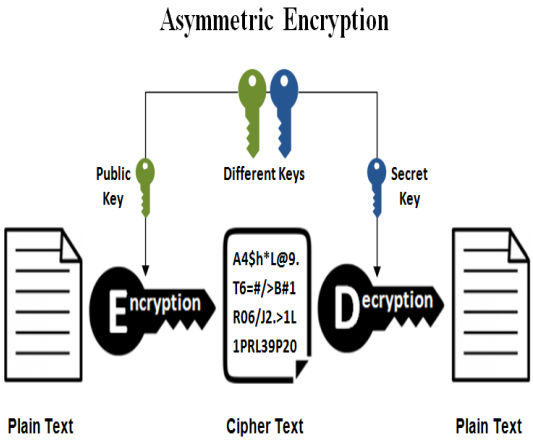
Kerberos as a solution to these network security problems. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to prove their identity, they can also encrypt all of their communications to assure privacy and data integrity as they go about their business.



Symmetric Encryption: Both encryption and decryption of data use the same secret key. Symmetric cryptography is also known as secret key cryptography.



Asymmetric encryption: Two different keys are used for encrypting and decrypting the data. The public key encryption technique is the primary example of this using a "public key" and a "private key" pair. Therefore, it is also referred as public key cryptography.



	Normal Flow	Under Attack	After Encryption
End-to-End Delay (ms)	18.22	35.25	19.09
Throughput (bps)	170099.91	65072.06	143440

The comparative analysis if the grid is under attack and after the Encryption applied on the grid.

IV. 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.

I have simulated a simplified model and simulated various grids before attack and after the encryption

algorithm is applied to that particular grid. As shown in the graphs the packets are increasing and the throughput of the nodes increased incredibly after the encryption algorithms are applied to the grid. Further, it has been shown that, randomly and dynamically 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.

REFERENCES

1. Foster, I. (2002). 'What is the Grid? A Three Point Checklist', GridToday, Vol.1, No.6.
2. Ann Chervenak, Ewa Deelman, Carl Kesselman, Bill Allcock, Ian Foster, Veronika Nefedova, Jason Lee, Alex Sim, Arie Shoshani, Bob Drach, Dean Williams,Don Middleton, (2003), 'High-Performance Remote Access to Climate Simulation Data: A Challenge Problem for Data Grid Technologies', Parallel Computing, Special Issue : High Performance Computing with geographical data, ACM Press, Vol.29, Issue 10, pp.1335-1356.
3. Antonio Carzaniga, Matthew J. Rutherford, Alexander L. Wolf, (2004), 'A Routing Scheme for Content-Based Networking', IEEE conference on Computer and Communications (INFOCOM' 04), pp.918-928.
4. Marty Humphery, Mary R. Thomson, and Keith R.Jackson, (2005), 'Security for Grids', Proceeding of the IEEE, Vol.93, No.3, pp.644-650.
5. GARUDA Project , www. garudaindia.