International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 9 2670 – 2675

New Enhance Approach Based on RC4 for the Grid Security

Navjeet Singh Chehal
Department of Computer Science & Engineering
Adesh Institute of Engg. & Technology
Faridkot, India
navjeetsinghchahal@gmail.com

Naseeb Singh
Department of Computer Science & Engineering
Adesh Institute of Engg. & Technology
Faridkot, India

Abstract- Grid computing applies resources of many computers in a network to solve one problem at the time. Grid computing can be like a distributed and large scale cluster computing or a parallel processing .Grid is nothing but prototyping a computational grid for infrastructure and an access grid for people. Grid computing is cost effective for a given amount of resources. To solve problems this requires enormous amount of computing power. Resources of many computers can be synergistically harnessed and managed to achieve a common objective.

Security Issues in Grid system

1) Protect application and data from system where computer executes.
2) Stronger Authentication needed.
3) Protect local execution from remote system.
4) Different security policies.

Grid computing is about several processors distributed globally and sharing the computational resources to solve various problems. Securities in grid computing are a very hot topic of research now a day. The major issues associated with Grid computing are co-coordinating resource sharing and security measures. There are number of approaches over the grid and other network application is RC4 but there are many weaknesses in RC4 so a new enhanced approach is proposed in this paper. The main working of research work is to enhance the security of RC4 for making it stronger than the previous RC4. RC4 algorithm is a two stage process for encryption and decryption i.e. KSA & PRGA. In proposed algorithm ,we generated two additional random matrix temp2[ ] ,temp3[ ] ,which is generated from two sub keys lenths,which generated from the inputting key lenths.These two matrices apply in both the stages of the RC4 to generate both the index as well as generate the random byte values.

Index Terms*-Grid computing, Distributed computing,RC4 (Rivest Cipher 4). KSA (Key scheduling Algorithm), PRGA (Pseudo Random Generator Algorithm).*

*****

1. INTRODUCTION

1.1 Distributed computing: A distributed computer system consists of multiple software components that are on multiple computers, but run as a single system. The computers that are in a distributed system can be physically close together and connected by a local network, or they can be geographically distant and connected by a wide area network. A distributed system can consist of any number of possible configurations, such as mainframes, personal computers, workstations, minicomputers and so on. The goal of distributed computing is to make such a network work as a single computer.

A distributed system consists of multiple autonomous computers that communicate through a computer network. The computers interact with each other in order to achieve a common goal. Distributed computing also refers to the use of distributed systems to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which is solved by one or more computers [4]. Distributed computing systems can run on hardware that is provided by many vendors, and can use a variety of standards-based software components. Such systems are independent of the underlying software. They can run on various operating systems, and can use various communications protocols. Some hardware might use UNIX(R) as the operating system, while other hardware might use Windows operating systems.

1.2 Cloud computing: Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service [2].The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more inefficient computing by centralizing storage, memory, processing and bandwidth.

1.3 Grid computing: Grid computing can be seen as a journey along a path of integrating various technologies and

solutions that move us closer to the final goal. Its key values are in the underlying distributed computing infrastructure technologies that are evolving in support of cross-organizational application and resource sharing—in a word, virtualization—virtualization across technologies, platforms, and organizations. This kind of virtualization is only achievable through the use of open standards. Open standards help ensure that applications can transparently take advantage of whatever appropriate resources can be made available to them.

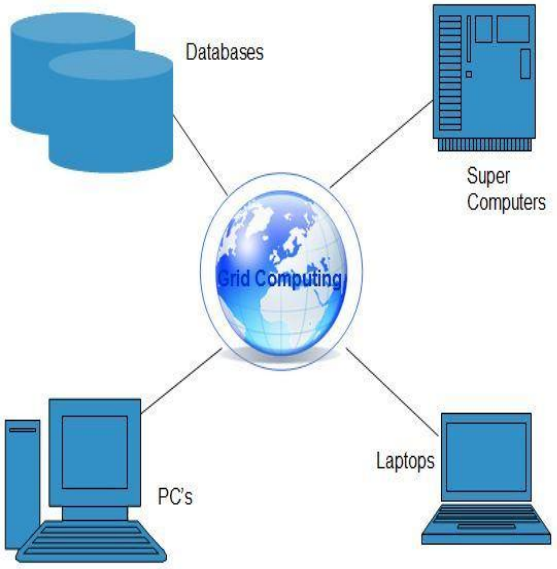


Figure1.1: Grid Computing

Grid computing is applying the resources of many computers in a network to a single problem at the same time - usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data. A well-known example of grid computing in the public domain is the ongoing SETI (Search for Extraterrestrial Intelligence) @Home project in which thousands of people are sharing the unused processor cycles of their PCs. The grid can be thought of as a distributed system with non-interactive workloads that involve a large number of files [1]. Grids are a form of distributed computing whereby a "super virtual computer" is composed of many networked LOOSELY coupled computers acting together to perform very large tasks. This technology has been applied to computationally intensive scientific, mathematical.

Grid computing appears to be a promising trend for three reasons:

(1) Its ability to make more cost-effective use of a given amount of computer resources.

(2) A way to solve problems that can't be approached without an enormous amount of computing power, and

(3) It suggests that the resources of many computers can be cooperatively and perhaps synergistically harnessed and managed as collaboration toward a common objective.

Grid computing makes more resources available to more people and organizations while allowing those responsible for the IT infrastructure to enhance resource balancing, reliability, and manageability [3].Grid computing is a processor architecture that combines computer resources from various domains to reach a main objective. In grid computing, the computers on the network can work on a task together, thus functioning as a supercomputer.

1.4 Areas of Grid computing:

1. Security
2. Resource management
3. Data management

1.5 Cloud Computing versus Grid Computing

For some, the comparison between these two types of computing could be hard to understand since they aren't much exclusive to each other. Rather, they are used for enhancing the utilization of the available resources. Furthermore, they both use the concept of abstraction at an extensive scale, each having distinct elements which interact with each other. The only differentiating factor between the two is the method it adopts for computing the tasks within their individual environments. In grid computing, a single big task is split into multiple smaller tasks which are further distributed to different computing machines. Upon completion of these smaller tasks, they are sent back to the primary machine which in return offers a single output. Whereas, a cloud computing architecture is intended to enable users to use difference services without the need for investment in the underlying architecture. Though, grid to offers similar facility for computing power, but cloud computing isn't restricted to just that. With a cloud users can avail various services such as website hosting etc [2].

In grid computing, a single big task is split into multiple smaller tasks which are further distributed to different computing machines. Upon completion of these smaller tasks, they are sent back to the primary machine which in return offers a single output. In the environment of Cloud Computing, users get a single interface for multiple servers. Cloud is basically an extension to object oriented programming concept of abstraction. It eliminates the complex working details from being visible to the users. What users can view is just an interface, which only involves receiving the inputs and providing the outputs. The process involved in generating the outputs is completely invisible. Rather, they are used for enhancing the utilization of the available resources. Furthermore, they both use the concept of abstraction at an extensive scale, each having distinct elements which interact with each other. Grid systems support large set of users organized in virtual organizations, Cloud systems support individual users [3].

The difference between grid computing and cloud computing is hard to grasp because they are not always mutually exclusive. In fact, they are both used to economize computing by maximizing existing resources. Additionally, both architectures use abstraction extensively, and both have distinct elements which interact with each other.

However, the difference between the two lies in the way the tasks are computed in each respective environment. In a computational grid, one large job is divided into many small

portions and executed on multiple machines. This characteristic is fundamental to a grid; not so in a cloud [6].

The computing cloud is intended to allow the user to avail of various services without investing in the underlying architecture. While grid computing also offers a similar facility for computing power, cloud computing isn't restricted to just that. A cloud can offer many different services, from web hosting, right down to word processing [7]. In fact, a computing cloud can combine services to present a user with a homogenous optimized result.

2. SECURITY IN GRID COMPUTING

Cryptography approaches are used to provide the security of data and information over the Network during transmission of data. In the Cryptography various algorithms are provided the various Security Services like Confidentiality, Data Integrity, Authentication to protect against the attacks, for examples: - release of message contents, modification of message, masquerade etc[1]. All the attacks are further categories under the two categories, Active and Passive attack. Active attack is where attacker after accessing the message attempts some modification over the message likes modification of message. In passive attack is where attacker just accessing the message not done the modification over the message contents likes release of message contents. In Cryptography numbers of algorithms are used to provide the Security Services. The Cryptography algorithms are dividing into the two classes, Symmetric and Asymmetric encryption. Symmetric encryption is known as Single key encryption or Secret key encryption or Private Key encryption. In the Secret key encryption, during the encryption and decryption same secret key (same key) is used to convert the plaintext into the cipher text and cipher text into the plain text [4]. In the Asymmetric encryption (Public key Encryption), during encryption and decryption two keys (Pair of keys) are used for encryption and decryption, one of the key is known as public key and second key is known as private key. The Symmetric Encryption class is important in modern Cryptography, reason being the Symmetric encryption Cryptosystem is faster as compare to the Asymmetric encryption cryptosystem [5].

RC4 stream cipher most preferred Stream cipher algorithm. In the RC4 algorithm, there are two stages process during encryption as well as decryption. The algorithm is dividing into the two parts KSA (Key scheduling Algorithm) and PRGA (Pseudo Random Generator Algorithm).[8] KSA as the first stage of algorithm also knows as initialization of S (s is state vector) and PRGA known as stream generation in the RC4 whole process of algorithm, mean RC4 basically two stages process. In the first stages of RC4 Stream Cipher algorithm on the bases of variable sized key from 1 to 256 a State Vector (State Table) of fixed length 256 bytes is generated, after on the base of State Table, we generate the key stream that XOR with plaintext and cipher text during encryption and decryption [9].

3. PROPOSED ALGORITHM

In present work security is discuss in context to the grid computing. Grid Computing is the most favors distributed computing. On the grid, there are lots of thing we have to manage like: data management, policy management and the most important among them is the security management. Security management is the one of the important task needs to manage over the grid. There are various security services needs to manage on the grid from the security concern like: authentication, authorization and the important among them all is the confidentiality. Now to manage the confidentiality over the grid, there are numbers of approaches being used like: DES, AES. But the most used approach over the grid and other network application is the RC4.RC4 algorithm is the two stages process for encryption and decryption, KSA and PRGA. The weaknesses are found in the both stages of RC4 algorithm after analyzing these weaknesses it is proposed in the present work to design **"New enhance approach based on RC4 for the Grid Security"**. The main working of research work is to enhance the security of the RC4 for making it stronger than the previous RC4 stream.

3.1 Proposed Algorithm

KSA:

1. Input one Keys (Key Lengths)
2. Generate the two sub keys
3. Initialize the three Key[length] // generate on the bases of two sub keys
   For i=0 to length
   Key1 [i]=random value;
   Next
   For i=0 to length
   Key2 [i]=random value;
   Next
   For i=0 to length
   Key3 [i]=random value;
   Next
4. Initialize the three Temporary Matrix
   For i=0 to N
   Temp1 [i]= value
   Temp2 [i]= value
   Temp3 [i]= value
   Next
5. Initialize the State Matrix
   For i=0 to N
   S1 [i]=i;
   Next
6. Permutation on State Matrix
   j1=j2=0
   For i=0 to N
   J1=(j1+s1[i]+s1[j1]+temp2[i]+temp2[j1]+temp1[i] +temp1[j1] +temp3[i]+temp3[j1])%N;
   Swap (s1[i],s1[j1])
   Next

PRGA:

7. Generate the random values used for encryption
   i=j1=j2=j3=0
   While (T)
   i=i+1 % N

 ISSN: 2321-8169
2670 – 2675

j1=j1+s1[i]+s[j1]+temp2[j1]+
temp3[j1]+temp2[i] +temp3[i] % N
Swap (s1[i],s1[j1])
index1=(s1[i]+s1[j1]) % N
output1= s1[index1]
CT= PT1 XoR output1
Wend (End While)

In proposed algorithm, for securing the RC4 algorithm and further two stages of RC4 stream cipher KSA and PRGA, we generated two additional random matrix temp2[ ], tempp3[ ], which is generated from the sub two key lengths , which generated from the main inputting key lengths. These two matrices apply in both the stages of the RC4 to generate the index as well as generate the random bytes values.

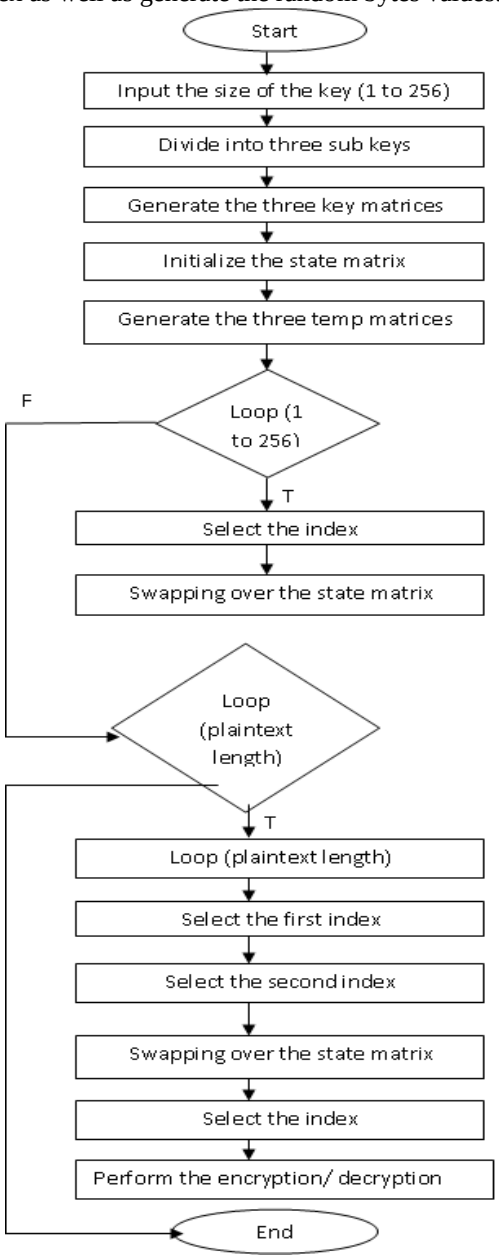


Figure 3.1: Flowchart of Proposed Algorithm

4. RESULTS AND DEMONSTRATION

RC4 Algorithm Output:

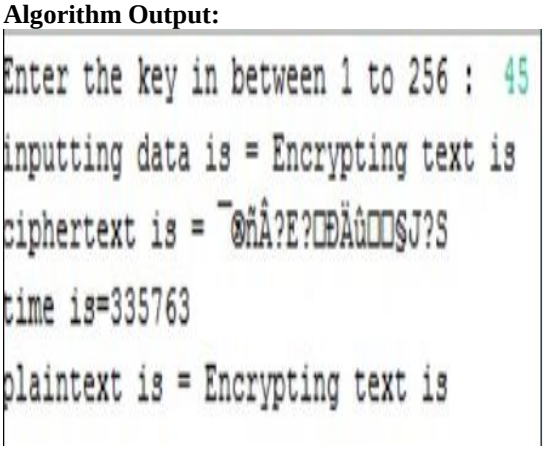
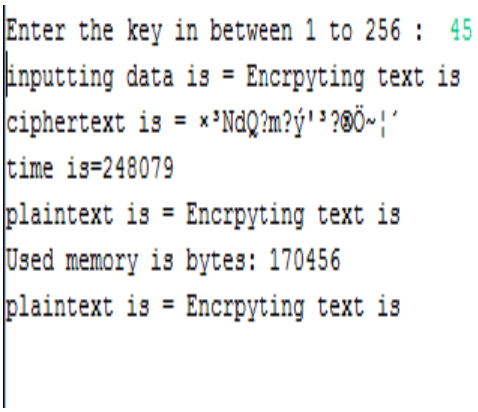


Figure 4.1: RC4 Algorithm Output

Proposed Algorithm Output:



Although time taken by proposed algorithm is more than the existing algorithm but the proposed algorithm is more secure than the existing one.

Analysis of the Algorithm:

Now we are going to discuss the analysis result of the algorithms.

The parameters on which we have analyzed the algorithm are as follows:

1. Encryption time
2. Memory

1. Encryption time

In this section we presents the evaluation time of the algorithm taken during encryption of the data. To calculate the encryption time we assume Keylen= 200

RC4 Algorithm

Table 4.1:RC4 Encryption Time

Data(Bytes)	Encryption Time
10	86044
20	93054
30	107506
40	114505
50	127679

4.2 Proposed Algorithm:

Table 4.2: Proposed Algorithm Encryption Time

Data(Bytes)	Encryption Time
10	140754
20	158686
30	168532
40	175235
50	187992

Simulation Result:

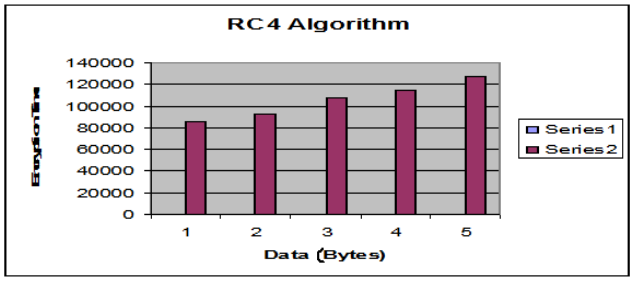


Figure 4.3: RC4 Encryption Time

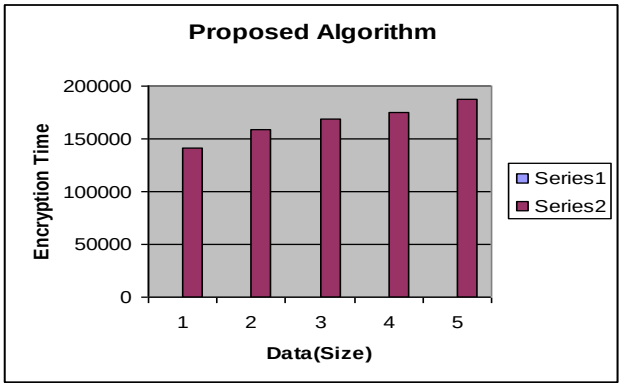


Figure 4.4: Proposed Algorithm Encryption Time

2. Memory

In this section, we are going to discuss the analysis of the both RC4 and proposed algorithm on the basis of Memory utilize by both the algorithms. For this evaluation, taking the data size=10 bytes and keylen=200.

Table 4.3: Memory Utilization

Name of Algorithm	Memory in Bytes
RC4	209704
Proposed Algorithm	209856

Memory Utilization Comparison:

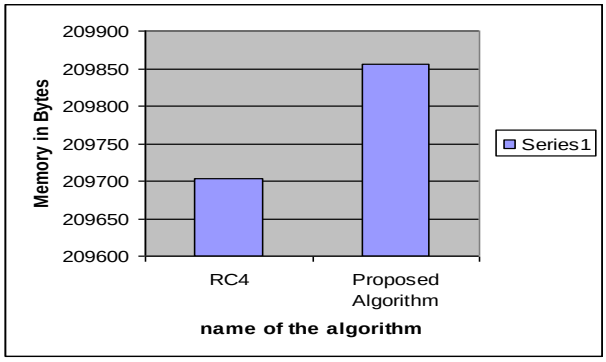


Figure 4.5: Memory Utilization

5. CONCLUSION AND FUTURE SCOPE

In present work, we describe the enhanced approach to secure the RC4 algorithm which is already used over the grid computing for securing the grid. To enhance the RC4 algorithm we introduce the three temp matrices to do the randomization on the state matrix in the KSA stage of the proposed algorithm. In proposed algorithm the output of the KSA stage is not only the state matrix but also the two temp matrices that are given to the PRGA stage of the algorithm that is used to provide the high level of randomization on the state matrix. The Previous RC4 algorithm having lots of attacks, so data over the grid not to be secure. So to solve these problems, the proposed algorithm is design for securing RC4 and the Grid environment.

In future work the RC4 algorithm is most used algorithm. So to enhance the algorithm, number of researchers proposed the various algorithms. So with the enhancement in present work, does not mean that the enhancement work stop now over RC4, still if any other researcher having any idea regarding to improve the security of the algorithm, then will be apply over the RC4 stream cipher.

REFERENCES

[1] Chhattar Singh Lamba "Design and Analysis of Stream Cipher for Network Security" ICCSN '10 Proceedings of the 2010 Second International Conference on Communication Software and Networks on page no 562-567, 2010.

[2] Harmeet Kaur"*Comparison of Security in Grid and Cloud Computing"*, International Journal of Research in Engineering and Technology, on page no 136-145Volume: 02 Issue: 09, Sep-2013.

[3] Jian Xie, Xiaozhong Pan "An improved RC4 stream cipher", Computer Application and System Modeling (ICCASM), 2010 International Conference in volume 7 page no.156-159, 22-24 Oct.2010.

[4] Kusum Yadav Rakesh Kumar, *"Security in Grid Computing"* International Journal of Advances in Engineering Research Vol. No. 1, May 2011.

[5] K.Anitha Kumari, G.Sudha Sadasivam, R.Senthil Prabha , G.Saranya "Grid based security for online trading", Process Automation, Control and Computing (PACC), 2011 International Conference on page no 1 – 4, 20-22 July 2011.

[6] Mehmet Hadi Gunes, Cansın Y. Evrenosoglu "Blind Processing: Securing Data against System Administrators", IEEE International Workshop on Management of Smart Grids on page no 301-302, march 2010.

[7] M.ali, Z.Y.Dong, "A grid computing based framework for power system reliability and security analysis" IEEE International Conference for security on grid, 2010.

[8] Tiezhu Zhao, *Shoubin Dong "A* trust aware security model for multi domain grid", The Fifth Annual ChinaGrid Conference Guangzhou, Guangdong China on page no.43-47, July 16-July 18, 2010.

[9] Sanjeev Puri *"Deliberate Secure Grid Computing Blueprint Design in Indian Context"* Computer Network and Information Security, Published Online June 2012 (http://www.mecs-press.org/) .