Abstract-Grid computing is about several processors distributed globally and sharing the computational resources to solve various problems. Grid computing has become an increasingly important research topic within computer science as in academic educational purpose and industrial research to government sector. Grid computing is concerned how to share and coordinated use diverse resources in distributed environments. The dynamic and multi-institutional nature of these environments introduces challenging security issues, which include integration with existing systems and technologies, interoperability with different “hosting environments” and trust relationships among interacting hosting environments. The major issues associated with grid computing are coordinating resource sharing and security measures. We need new technical approaches to handle those security issues. Security solution consist of ARC4 (Rivest Cipher 4) algorithm combined with Advance encryption standard (AES) which provides solution for security with whitener (Whitening is used to enhance the security of the cipher). In related study hybrid solution has been proposed but has some overhead while processing security for large distributed networks. In current technology with development of smart grid architecture, we need less overhead to use best resources in grid computing. So in this research we will propose an enhanceamalgamencrytption solution using AES and RC4 which can overcome overhead and security limitations.

Keywords: -Grid Computing, Security, Advance encryption standard (AES), Rivest Cipher 4 (RC4).

1 - Introduction

Computing Environment is a collection of homogeneous and heterogeneous computers, software, and the networks which support the processing and exchange of information in order to support various types of computing solutions. The main three computing environment are Distributed computing, Cloud computing and Grid computing.

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 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 personal computers, workstations and so on. The major 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 to achieve a common goal. Distributed computing also refers to the use of distributed system to solve computational problems. In distributed computing, a problem is divided into many tasks, each of which solved by one or more computers. Distributed computing system 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.

1.2 Cloud Computing :

Cloud computing is a general term for anything that involves delivering hosted services over the internet. These services are divided into three categories: Infrastructure-as-a-Service, Platform-as-a-Service and Software-as-a-Service. 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 efficient computing by centralizing, storage, memory, processing and bandwidth. An Example of cloud computing is Yahoo e-mail, Gmail etc. Just user need an internet connection and can send and receive emails. The server and email management software is all on the cloud and is totally managed by the cloud service provider Yahoo, Google etc. Cloud computing comes into focus only when you think about what IT always needs: a way to increase capacity or add capabilities on the fly without investing in new infrastructure training new personnel, or licensing new software. Cloud computing encompasses any subscription-bases or pay-per-use service that, in real time over the internet, extends IT’s existing capabilities. Cloud computing, mostly referred as simply “the cloud” which is the delivery the on-demand services and computing resources everything from applications to data to the centres over the Internet.

1.3 Overview of Grid Computing

Grid computing involves integration, virtualization, management of services, and resources in a distributed, heterogeneous environment which includes the collections of different users and resources across different organizational domains. Grid computing is applying the resource of many computers in network to a single problem at a same time –
usually to scientific or technical problem that requires a great number of computer processing cycles or access to large amount of data. So grid computing can be useful in many ways as:

- **Large scale**: Grid is able to deal with the many of resources ranging from a few to millions.
- **Geographical distribution**: Grid’s resources can be located at different locations.
- **Heterogeneity**: It is heterogeneous in nature. Software, hardware resources data, programs and networks can be vary.
- **Resource sharing**: Resources in a grid are belonging to different organizationsthat allow other organizations (i.e. users) to access their resources under secure environment. Each organization may be have its own different securityand administrative policies so it also require the proper administrative management
- **Quality of Service (QoS)**: High levels of performance standard of services, failure handling , security , monitoring etc. are the key to maintain the QoS.

In Grid computing, when many computers are interconnections and all working together on a single common problem to achieve a particular goal is known as **Grid Computing**. Grid computing is use for the coordinating and sharing of different resources in distributed ‘virtual organizations’. A **virtual organization** (VO) means a set of individuals or institutions group which are sharing the resources under some rules and conditions. All these “virtual organizations” may differ in size, structure, duration,and scope. So In Grid computing the systems and applications are used to integrate and manage resources and services within distributed, heterogeneous, ‘virtual organizations’ [1].

As already mentioned, the definition of a grid is somewhat subjective. According to “Foster” and “Kesselman” a grid is a that conforms to three specific categories:

- It coordinates resource that is not subject to centralized control
- It uses standard, general purpose protocols and interfaces,
- it delivers nontrivial QoS
  Like: response time, availability, throughput, security

![Figure 1-1 Grid environment](image1)

On the other hand kon et al. define that Grid computing as “coordinated resource sharing and problem solved in dynamic , multi-institution virtual organizations
Therefore, the following descriptions of various kinds of grids must be taken. Grids can be built in all sizes, ranging from few machines in a department to groups of machines organized as a hierarchy spanning the world. As presented in Figure 1-2, the simple grid which is having a few computers, all of the same hardware architecture and same operating system that are connected on a local network. This kind of grid uses homogeneous systems so there are fewer considerations and may be used for specialized applications. These machines are mostly in one department of an organization, and the use of that grid may not require such special policies or high security levels. Because the machines have the same architecture and operating system, the selective application software for these machines is usually simple. So people would call it as a **cluster implementation rather than a grid**.

![Figure 1-2 Virtual organization environment](image2)
1.4 Grid applications services:-
As in grid-architected services continue to be developed, a grid applications that use one or more grid architected services. Therefore, these applications comprise the main layer of the Grid architecture. The Grid capabilities share and build on a number of common components which include Infrastructure, Execution management, Data, Resource management, Self-management, Security and Information services[1].

- **Grid middleware Infrastructure Services:** It enable bulk data communication between different resources (computer, storage, application, etc.) also removing barriers associated with shared utilization.
- **Execution Management Services:** Execution Management Services (EMS) enables grid applications to have coordinated access to underlying resources which include CPU, disk, data, memory, and services-regardless of their physical locations or access mechanisms.
- **Data Services:** These Grid services concerned with the management of access to and update of data resource, that are along with transfer of data between resources. These are collectively called ‘data services’. The ‘data service’ can be used movement of data where it is needed-managing replicated copies, run queries execution and updates, and transforming data into new formats if required.
- **Resource Management Services:** In a grid, the resource management services enables the monitoring, reservation, deployment, and configuration of grid resources based on seamless quality of service (QoS) requirements.

**Figure 1-3 Grid application services[1]**

- **Security Services**
  Grid security services facilitate the enforcement of the security-related policy within virtual organizations, promoting safe resource-sharing and appropriate authentication and authorization of users that span multiple domains. Each domain has its own business objectives and translates in an enforced security policy.
- **Self-management Services**
  Self-management service supports the attainment of the stated levels of service with as much automation as possible, aim to reduce the cost and complexity of managing the system.

1.5 Layered Architecture:-
The Grid is currently working to define these architected grid services in areas like program execution, data services, and core services. In which part of them has been defined, and some implementations have already appeared. As newly architected services begin to appear, Grid will become a more useful Service-Oriented Architecture (SOA)[1]

- **Fabric.** The lowest layer job is used to make a common interface on all possible kinds of resources available. Access by upper layers which is granted via standardized processes. All resources on which is applicable, that can be integrated in grid concept. This contains computers, storage systems, networks or sensors.

**Figure 1-4 Resource management**

**Figure 1-5 Grid Architecture[1]**
Resource and connectivity protocols: The connectivity layer defines the basic communication- and authentication protocols which are needed by the grid. While the communication protocols allow the exchange of files between different resources connected by first layer, and authentication protocols allow to communicate confidentially and to ensure the identity of the two partners. This contains observation, initiation, clearance, control and negotiation of security parameters.

Collective services: The purpose of this layer is the coordination of multiple resources. Access of these resources does not happen directly but merely via the underlying protocols and interfaces. So the job of this layer contain among others the creation of a directory service, they supply diagnostic, monitoring and file replication services.

User applications: To this layer belong all those applications which are operating in the environment of a virtual organization. Jobs at the lower layers get called by the applications and can use resources transparently.

1.6 Security Issues in Grid Computing:-

Security challenges in a grid environment[3]:

Integration

The grid security infrastructure is required to integrate with existing security infrastructures across platforms and hosting environment. The over-all grid security architecture is required to implementation agnostic and be extensible to incorporate new security services as they become available.

Interoperability

Grid services which traverse multiple domains and hosting environments need to be able to interact with each other to allow domains to exchange messages (for example, via SOAP/HTTP), allow each party to specify security policy applied to a secure conversation, and provide mechanisms to identify a user from one domain in another domain.

Trust Relationship

Grid service request can span multiple security domains. That security domains involved to meet Grid service request require establishing trust with each other. Because of the dynamic nature of grid environment it is unfeasible to establish end-to-end trust prior to execution of an application. So the issue related to trust establishment becomes more complicated with transient Grid services.

Figure 1-6 Grid security model [1]

1.7 Security requirements:-

Security requirements within the Grid environment are driven by the need to support dynamic, scalable, distributed virtual organizations (VOs) [4]—collections of diverse and distributed individuals that seek to share and use diverse resources in a coordinated fashion. From the security perspective, the key attribute of VOs is that participants and resources are governed by the rules and policies of the classical organizations of which they are members. Furthermore some VOs, such as multiyear scientific collaborations may be large & long-lived (in which case explicit negotiations with resource providers are acceptable) other will be short-lived created, perhaps to support a single task, e.g. the two individuals sharing documents and data as they write a proposal—in which case overheads associated with VO creation and operation have to be small. So the different grid computing systems have the vulnerabilities as under.

<table>
<thead>
<tr>
<th>Type of grid computing system</th>
<th>Brief explanation</th>
<th>Most common vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computational grid</td>
<td>Grid architectures that focus on setting aside resources specifically for computing power; i.e. solving equations and complex mathematical problems; machines participating in this type of grid are usually high-performance servers.</td>
<td>Programs with infinite loops can be used to bring down nodes of this grid, decreasing functionality</td>
</tr>
<tr>
<td>Data grid</td>
<td>Grid architecture responsible for storage and providing access to large volumes of data, often across several organizations</td>
<td>Users can overwrite data of other users if they exceed their available space-thiscorrupts the other users’ data</td>
</tr>
<tr>
<td>Service grid</td>
<td>A grid which provides services that are not available on a single machine</td>
<td>Users can use the service grid to launch Denial of Service Attack (DOS) against another site</td>
</tr>
</tbody>
</table>

Table 1: vulnerabilities in different grid computing systems [13]
1.8 Cryptography:
To overcome this, cryptography approaches are used to provide the security of data and information over the network during transmission of data. In this technique various algorithms provide different security services, such as data integrity, confidentiality, authentication etc. which are all protects against the intruder. Intruder is an attacker who can do modification in message and release messages on user’s behalf. Intruder can attack in so many ways on user’s system to harm them and get the benefits in different ways like to hack some one’s web site or user’s bank account no. and password so he can transfer the money easily. If intruder successfully attacks the system he can access user or organization’s vital information which can be lead to a great lose for an organization. All the attacks are further divided into two categories:

- **Active Attacks**: The attack is active when it attempts to alter system resources and try to affect their operation so it compromises with integrity and availability.
- **Passive Attack**: These are attempt to learn and make use of information from the system but does not affect any system resources: so it compromises with confidentiality.

Cryptography is the science of encrypting a plaintext, such that it is rendered unreadable to others except the person for whom the message is intended. It involves two processes of encryption and decryption.

- **Encryption**: The process of “encryption” converts the plaintext into encrypted form, which is known as the cipher text.
- **Decryption**: The process of “decryption” converts the cipher text into the original plaintext.

The algorithm which contains encryption decryption processes is known as a cipher. In simple words, all that a cipher has to do is replace a piece of information with something else. The replacement follows a set of rules or it would not be possible to easily get it back to the original form and the intended recipient would not be able to read the message.

The rules used are central to a unique object called key. This key is used in the encryption process and the same key has to be used in the decryption process in order to generate the plaintext[2].

The Cryptography algorithm is divided into two classes, Symmetric and Asymmetric encryption.

- **Symmetric encryption**: Is known as single key encryption or secret & private key encryption. In this process, during the encryption/decryption same secret key is used to convert the plaintext into the cipher text and cipher text into the plaintext.
- **Asymmetric encryption**: Whereas in asymmetric encryption, during encryption two keys are used one is public key and second is private key.

The Symmetric encryption technique is more important than asymmetric one the reason behind is the Symmetric encryption is faster as compare the Asymmetric encryption cryptosystem. The Symmetric encryption algorithms are divided into two classes stream cipher and block cipher.

- **Stream cipher**: These algorithms crypt & decrypt the data bit by bit, byte by byte, character by character that means the encryption decryption process to convert the plaintext into cipher and further cipher text into plain text is done bit by bit, byte by byte or character by character. In streaming process one bit or character is encrypt or decrypt at a time.
- **Block cipher**: The encryption and decryption is done in blocks, algorithm divides the data into specific block size (16 bytes, 32 bytes, 64 bytes, 128 bytes) depending on the algorithm requirement. After the complete block encrypt and decrypt at a time means it can do encryption and decryption more than one character in a fixed length block manner.

1.9 **Advance Encryption Standard**:--
AES is a symmetric-key algorithm (same key is used in both encryption and decryption) and based substitution-permutation design that makes AES so secure against attacks. It is a block cipher which means it breaks data in blocks and combines key with each to get encrypted data[2].

AES has transformation rounds which are called a definite number of times to encrypt data depending on the bit length of the key used in the algorithm i.e. 10, 12 or 14 rounds are used for 128, 192 or 265 bit key respectively. The rounds can be called in the reverse manner to decrypt the cipher text.
Figure 1.8 Advance Encryption Standard[2]

AES is based on a design principle known as a substitution-permutation network. It is fast in both software and hardware. The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect the data or information. AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) the information. Encryption converts the data into an unintelligible form called cipher text which is unable to understand; decrypting the cipher text converts the data into its original form called plaintext.

Implementation of AES:
- **Key Expansion:** Round keys are generated by using the cipher key.
- **Initial Round:**
  - **AddRoundKey:** Bytes are combined with the round key using bitwise XOR.
- **Rounds**
Sub Bytes: A non-linear substitution step in which each byte is replaced with another byte according to an “S” table.

Shift Rows: In this each row is shifted cyclically a certain number of steps.

Mix Columns: Mixing operation operates on the columns which combining the four bytes in each column.

Add Round Key

Final Round (without MixColumns)
- SubBytes, ShiftRows&AddRoundKey

Rivest Cipher 4 (RC4):
“RC4” is a symmetric key cipher like AES. It is a stream cipher which means that the random key generated in RC4 is applied to each bit of the plaintext one at a time to get the encrypted text. As RC4 is a stream cipher, symmetric key algorithm [2]. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bits to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the cipher text.

The steps for RC4 encryption algorithm is as follows [19]
- Get the data for encryption and then select the key.
- Createtwo strings of arrays.
- Initiate one array with the numbers from 0 to 255.
- Fill the other array with selected key.
- Randomize first array depending on the array of the key.
- Randomize first array within itself to generate final key stream.
- XOR final key stream with data to be encrypted to give cipher text.
With the growing trend of using computers and internet for all purposes, sending data securely has become highly risky. Hence, security is the growing need of the day which stream ciphers like Rc4 are unable to provide. WEP application uses Rc4 but weaknesses in the Key Scheduling Algorithm of RC4 throws light on the risk factor. Studies show how knowing a few bits of the key in the Rc4 cipher, can easily break the cipher and determine the output of the cipher with a high probability. It was shown that for a cipher text attack, a key of arbitrary length could be easily recovered using this technique which renders the cipher highly insecure. AES has been suggested as a replacement on several occasions but AES being new and a block cipher, it is not as popular as Rc4. Moreover, AES is very slow compared to Rc4 which is one of the fastest ciphers known and is the major reason for its popularity. As security issues continue to arise, it is time to look at an alternate approach which is why the proposed algorithm can prove to be a cross between Rc4 and AES combining the characteristics of time and speed into a new cipher. Rc4 combined with AES is highly likely to create a secure algorithm. RC4 can be combined with AES in various ways. Related study also provides a hybrid solutions like limiting the rounds in AES combined with RC4 but due to overhead, we will try to increase more suitability along with more security for Grid networks.

II - PRESENT WORK

2.1 Present work:-
In this paper I have studied about Grid computing and focusing on security issues in grid computing and work on the encryption technique for which literature survey has been done. In the present research work we design the new security approach based on the combine properties of AES algorithm and RC4 algorithm. That is use over the grid computing environment which helps to prevention against the attacks and also to provide the better security solutions over the Grid environment. By this technique, it is possible to secure the various network applications like: Sensor Network, Wireless Network and other internet applications.

2.2 Scope of study:-
The future work has ample scope in the related area. Particularly talking about grid computing security, proposed solution can provide a secure communication for grid computing. Solutions which are already present are much appropriate for grid computing security because some provides security but increases the overhead which is not good for grid computing as grid is always about saving and managing the resources. Some of the security measures are less secure in term of large network implementation for smart grid networks. So the proposed solution will have great scope due to agile secure communication with less overhead than other techniques.

2.3 Problem formulation:-
In related study, hybrid solution for grid security has been proposed. It consist of combination of alteration in rivest cipher 4 algorithm by introducing temporary matrixes in the RC4. This make the security more complex and add security but if we consider large networks and smart grid environment applications, these changes are not suitable because it adds some complex conditions and more resources are required. To avoid complex calculations and to provide a suitable and strong encryption mechanism, combination of AES and RC4 can be a suitable solution. The key issue with AES is that it is a block cipher. Many blocks are encrypted with a single key, thus interrelating the blocks. If one block is managed to be broken, all others which share the common key can also be easily broken. Attack which is difficult against one block can be highly simplified when given multiple blocks with shared key. AES security depends on the permutation-combination transformations that are called a number of times. On reducing this number the speed of the cipher will increase but at the same time the security will decrease and the cipher will be more vulnerable to attacks. This vulnerability needs to be compensated by other changes in the algorithm. In our research work, we will implement a
hybrid algorithm with combination of RC4 and AES algorithms. We will use whitened plaintext from AES and output of AES will be act as input for RC4. The different blocks of the AES will have different Secret keys to provide strong security. Unlike the 10 rounds in the original 128 bit cipher, this has only 6 rounds with the first 5 rounds having all the permutation and transformation techniques of byte substitution, row shifting, mix columns, and then finally round key addition before moving to the next round. Round 6 in the hybrid is same as the round 10 in the original AES.

2.4 Objectives:

- To provide good solution for grid computing security by introducing secure hybrid architecture for AES and RC4algos.
- To provide solution for the overhead occurred while providing security in the grid computing.
- Use less CPU utilization time as compare to simple AES and Combine AES+RC4.
- Provide more security levels which are difficult to break down for an intruder.

(Whitened cipher level security, AES encryption security with two different Keys, RC4 encryption security Key)

2.5 Tools of data collection & analysis:-

For completion the desired work and successfully done the appropriate results I use “JAVA language” on “Net-Beans IDE” platform and then generate the graphs of the results by using the “YourKit JAVA Profiler” which is a Net-beans Add-ons. JAVA:Java is a programeing language used for simulating the environment. Java is a programeing language originally developed by James Gosling at Sun Microsystems and released in 1995as a core component of Sun microsystems’ Java platform. Java is a main standard for most of the Internet applications. It also provides the interactive processing and easy use of graphical applications and animation over the Internet. Since the Internet has the different types of computers and operating systems. A common language is needed to enable the computers to run programs that run on multiple plat-forms. This need was only fulfilled by the JAVA. It is an Object-Oriented language which is built on C and C++. It derives its syntax from C language & its features are influenced by C++ language. Java is used to create two types of programs. One is Applications and other is Applets.

- An Application is a program that runs on the user’s computers under the operating system.
- An Applet is a small window-based program which is run on HTML page using a java enabled web browser like Netscape Navigator, Firefox, Internet Explorer, or an Applet Viewer.

Java Features:-

- Compiled and Interpreter: -It has compilation & interpreter feature program of java which is first compiled the program and then it is to interpret it. First of all the program of java is compiled and after compilation the program it creates bytes codes instead of machine language. Then bytes codes are generated into the machine language with the help of the interpreter. So to execute the java program first compile it then it should be interpreter

- Platform independent: -JAVA language is platform independent that means program in java can easily be transferable. The concept is Write-Once-Run-anywhere is one of the key feature of JAVA programs. Which means the programs written on one platform can be run on any platform which must be having the JVM platform.

- Object-oriented: -It is an object-oriented language that all the codes of the java language are written into classes and objects. So it has the characteristics like Inheritance, Encapsulation, Polymorphism Dynamic binding, reusability and maintainability etc.

- Robust and secure: JAVA has the strong memory collection and automatic garbage collection mechanism it also provide the powerful exception handling and type checking mechanism as compare to other programing languages. Compiler check the program weather there is any error and interpreter checks any run time error and makes the system secure from crash. As security issues when we convert the code from one machine to another machine it first check code either it is effected by the virus or not and it also checks the safety of the code and if code contains any virus then it will not executedon the machine.

- Distributed: - JAVA is distributed language means because the program of java is compiled onto one machine can be easily transferred to machine and executes them on another machine because facility of bytes codes so java is specially designed for internet users which uses the remote computers for executing their programs on local machine after transferring the programs from remote computers or either from the internet. It helps programmers at remote locations to work together on a same project.

- Simple: -JAVA is a simple language because of it contains many features of other languages, like C & C++ and JAVA removes complexity because it does not use any pointers, storage classes & Go-to statements and JAVA also doesn’t support multiple inheritance.

- Interactive: - JAVA uses multithreaded techniques for execution and java is also called as interactive language because the code of java supports also Command user interface and Graphical user interface programs.

- Architectural neutral: -One of the key features of java which makes it different from other programming languages is it is architectural neutral (or platform independent). This means that program written on one platform can easily be run on other platform without having to rewrite or recompile them.

- Portable: -The portability actually comes because JAVA is architecture-neutral. In c/c++, source code may run differently on different hardware platforms. But in java, it has been simplified. Unlike C/C++, in JAVA the size of the primitive data types are machine independent.

- High performance: JAVA programs are faster than programs or scripts written in purely interpreted languages but slower than C & C++ programs that compiled to native machine languages.
2.6 Net-Beans IDE:-
Net-Beans is an open-source “Integrated Development Environment” (IDE) for developing with JAVA, C++, PHP & other programming languages. Net-Beans is coded in JAVA & runs on most of the Operating systems with Java Virtual Machine (JVM), including Mac and Linux. Net-Beans is an excellent IDE from Sun-Microsystems. Which means it is written in JAVA language and runs on all its major platforms.
Net-Beans (IDE) is an Open - source Integrated Development Environment. Net-Beans supports development of most of the JAVA application types (Java SE (including Java FX), Java ME, web and mobile applications) out of the box. Net-Beans use components which are also known as modules that are to enable software development. Net-Beans dynamically install modules & also allow users to download updated features. Net-Beans IDE modules include “Net-Beans Profiler”, a “Graphical User Interface” (GUI) design tool, and “Net-Beans JavaScript Editor”. All functions in“IDE” are provided by themodules. Each module provides the well-defined function such as supporting for the Java language and editing. Net-Beans contain all modules needed for Java development in a single download, which allowing the user to do work immediately. New features such as support for other programming languages can be also added by installing additional modules.
Net-Beans manage the platform features and components:
- User settings
- Net-Beans Visual Library
- Storage
- Integrated development tools
- Framework wizard

Net-Beans IDE Features:
- Fast & Smart Code Editing: An IDE is more than a text editor. The Net-Beans Editor matches words, indents lines, brackets and highlights source code syntactically & semantically. It also provides the templates, coding tips and different tools.
- Easy & Efficient Project Management: As clear overview of the applications with many folders & files and millions of lines code can become an easy task. Net-Beans IDE provides different views of the data from multiple project windows to helpful tools for setting up your applications & managing those efficiently and also letting you to scroll down into your data quickly and easily.
- Write Bug Free Code: - The cost of buggy code increases the longer it remains unfixed. Net-Beans provide static analysis tools especially for the integration with the Find-Bugs tool for checking, recognizing and then fixing common problems in JAVA code. In addition the Net-Beans Debugger helps you to place different break-points in the source code, add field watches, step through your code, run into methods, take snapshots & monitor execution when it occurs.
Net-Beans editor supports many languages from Java, C/C++, XML and HTML, to PHP, Groovy, Javadoc, JavaScript and JSP. Software has plug-in support for many other languages because of its extensibility feature.
- Code Bookmarks: This allows you to bookmark individual lines of code for easy browsing.
- Code Completion: If you are using visual studio, then you have seen this type of thing before. While coding you can pause and the code completion dialog box will appear. This works for the standard library items as well as items specific to user-created classes.
- Code Formatting: Net-Beans 6.1 give you the ability to customize every possible code formatting option. Each case is separated into group then each item in the group is a check-box. Changes are shows in real-time using a preview pane to the right. Once changes are made to these settings and after that when you are coding Net-Beans automatically accounts for them.
- Build Platform: Working with C/C++ project, you can select which platform to build the executable for.
- Single File Compile: Tired of building your entire project when all you want to do is make sure that the file you've just changed compiles cleanly? Net-Beans 6.1 offers the "Compile File" option to do just that.
- Favourites: Net-Beans 6.1 allow you to add files from your project to a list of Favourites. This is extremely helpful in large code bases.
- Symbol Tracking: While viewing source file, you just simply right-click on the symbol and you have option to track various things like the definition/declaration of symbol, its source/header file, all occurrences of symbol in the current file/entire project and more. Again, very helpful in large code bases.
- Include Directories: When developing a C/C++ project, Net-Beans 6.1 makes it easy to add additional include directories to its search path.
- Local History: It shows the history files.

2.7 YourKit JAVA Profiler:-
YourKit JAVA Profiler is development tool which analysis the dynamic performance at a run time. This tool helps to check the CPU and memory utilization.

- Benefits of YourKit JAVA profiler:-
- Powerful analysis capabilities: CPU time utilization and memory usage, memory leak detection, memory distribution reports and also has the reporting utility.
On-demand profiling: Means as per requirement user can enable profiling only when need it.
Free embedding into production: It is eligible to distribute a profiling DLL with the real-world applications without any extra charges.
J2EE support: It supports all the Java 5/6/7 versions.
Quick and easy installation: It is easy to install and User-friendly.

YourKit Java Profiler is a profiling tool that provides the most powerful, innovative and smart performance analysis capabilities. YourKit Java Profiler provides time savings tool.

- Quality: YourKit helps you to solve performance and scalability problems and ensuring the product quality. It has also the ability to perform run time.
- Productivity: Its users are enjoying massive productivity gains by having all of the advanced YourKit features at hand when they are needed most and by utilizing its seamless integration with the most popular IDEs and application servers.
- Time savings: By its unique on-demand profiling, user can run the profiled application without any extra overhead and can run actual profile when he needed. This functionality helps to save the developer's time.

III - RESULTS AND DISCUSSIONS

3.1 Proposed Enhanced Amalgam approach of AES-RC4:
AES and RC4 is the Hybrid Algorithm that I have proposed with the idea of the whitened Text. My Proposed algorithm starts with the having a plain text file and converting the content of the plain text file to the Whitened Text. This plain text file contains the actually the message that we want to encrypt.

- The whitened text conversion take place by converting our message to the Hexadecimal for “nd” then performing “XOR” with the Key that will be used for the encryption.

For Example Message is: Hello world, here is some sample text.
Whitened Text encryption: \[xU^U\]GYB_UYSEW_@E_UUATZBYB@MG

The Second step of the proposed algorithm comes with the AES (Advance Encryption Standard) Algorithm. The Basic difference between the AES and the proposed one is this that I am going to limit the number of the rounds that are basically 10, 12 rounds and more than that I am limiting them to “5 rounds” only. And I am providing the encryption of the AES not with only one key but with “Two keys” so that if being take place in between or any one is able to knows the one of the key the block encrypted with the other keys are saved. The algorithm starts with giving its whitened text as the input to the AES now this algorithm again encrypt the encrypted text.

The number of the step that is processed on each block is basically.

- Convert To State Array.
- Transformation
  - Add Rounds Keys.
  - Sub-Byte
  - Shift-Row
  - Mix Column
- Key Expansion

The Transformation is performed at each round on each block of the data. Our given input is firstly divided in to the block of the fixed size values. And then keys are applied to this.

E.g. now Input is: \[xU^U\]GYB_UYSEW_@E_UUATZBYB@MG
AES encryption is: \[E^t\mfw\,N/m\#hA\#ey\#jU\#^J\#]^%0;e

Now the final step of the algorithm will take place that is now I use this AES encrypted text as the input to the RC4. The algorithm processes the data in the form of the stream. RC4 generates a pseudorandom stream of bitsAs with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way (since exclusive-or with given data is an involution). To generate the key stream, the cipher makes use of a secret internal state which consists of two parts:

- A permutation of all 256 possible byte (denoted “S” below).
- Two 8-bit index-pointers (denoted “i” and “j”).

The permutation is initialized with a variable length key, typically between 40 and 256 bits.

This flow Diagram just shows the way our algorithm works.
Proposed Enhanced Amalgam approach of AES-RC4:

Simple AES (10 Rounds with single key):

CPU Time

Memory

Heap Memory

Figure 3.1: CPU time for Proposed AES+RC4

Figure 3.2: Memory used in Proposed AES+RC4

Figure 3.3: CPU Time for AES

Figure 3.4: Memory used in simple AES
Combine Simple AES+RC4:-

- Figure 3.5: CPU Time for AES + RC4
- Figure 3.6: Memory used in Combine AES+RC4

IV - Conclusion and Future Scope

4.1 Conclusion:-
In research we propose a secure communication for grid computing. Hybrid algorithm will be proposed by combining the flexibility of rivest cipher and strong security of AES algorithm. Each block of AES will have different security keys to make it stronger. This research will improve the secure communication in large structure based grid computing systems. Moreover in case of breaching into network, encryption provided by our proposed hybrid algorithm is very difficult to decrypt. That is use over the grid computing environment which helps to prevention against the attacks and also to provide the better security solutions over the Grid environment. By this technique, it is possible to secure the various network applications like: Sensor Network, Wireless Network and other internet applications.

4.2 Future Scope:-
The future has an ample scope in the related area of any Computing environment. In Grid computing the talk about security, the proposed solution can provide a secure communication for Grid computing. The proposed solution will have great scope due to agile secure communication with less overhead than other techniques. The field of cryptography is getting more advanced due to the upcoming trends in internet network and wireless. Further work is possible in this area by combining more such ciphers. Ciphers can be combined to make them more secure, more usable and effective. This technique can be further used in all spheres wherever encryption is needed. This paper discusses how to encrypt text securely within a short time using the hybrid cipher.

References