Volume 3, Issue 4, April 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Amalgam Encryption Approach for Grid Security: A Review

Kamal Jyoti
Department of computer science and engineering
Lovely professional university, India

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 a enhance amalgam encryption solution using AES and RC4 which can overcome overhead and security limitations.

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

I. Introduction

When many computers are interconnected and all working together on a single common problem to achieve a particular goal is known as Grid Computing. Grid computing is used 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 serviceswithin distributed, heterogeneous, 'virtual organizations', as in [1].

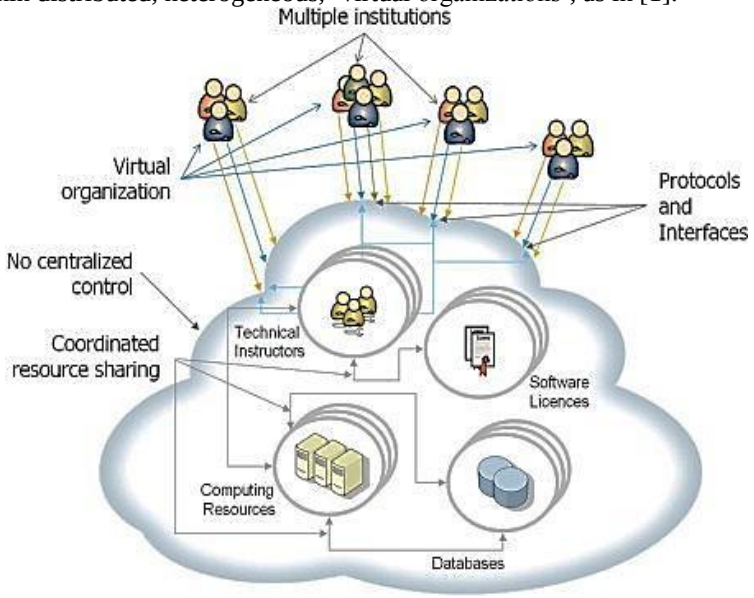

Fig. 1 Grid environment

As already mentioned, the definition of a grid is somewhat subjective. According to "Foster" and "Kesselman" a grid is conform 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

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.

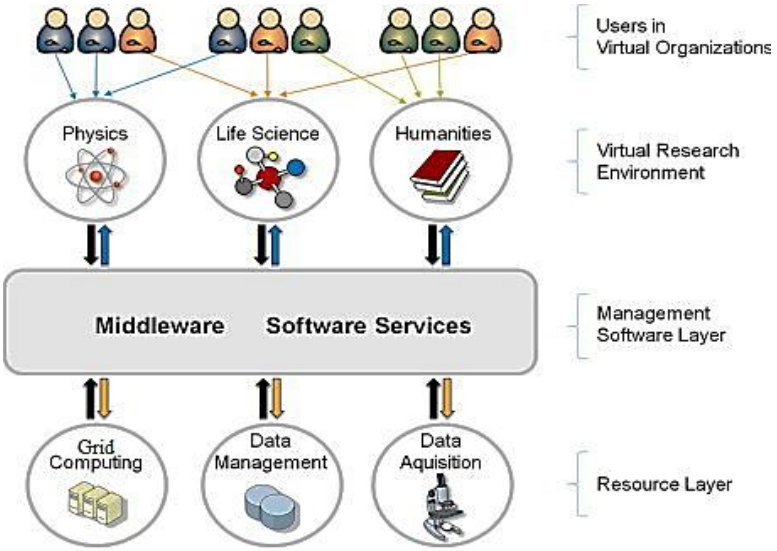

Figure 2 Virtual organization environments

A.Grid applications services:

As in grid-architected a service continues 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, security, self-management, and information services, as in [1].

- **Grid middleware Infrastructure Services: -**It enables 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.

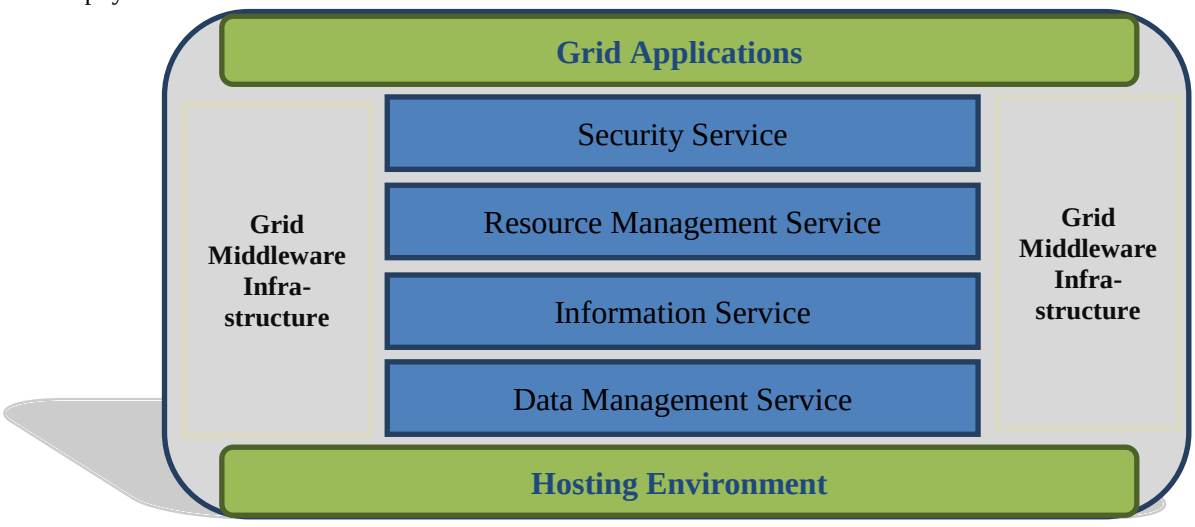

Fig.3 Grid application services

- **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.

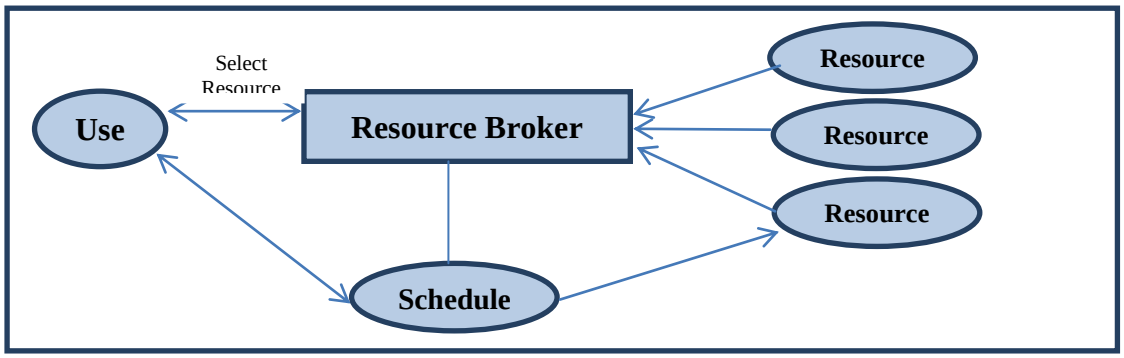

Fig.4 Resource management

- **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.

B. 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), as in [1].

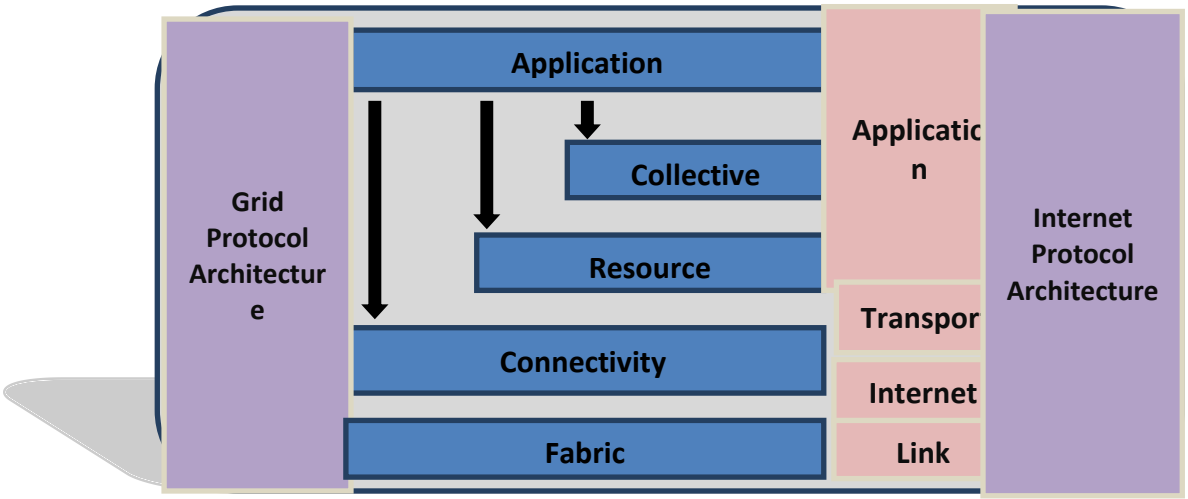

Fig. 5 Grid Architecture

- **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.
- **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 of the lower layers get called by applications and can use resources transparently.

C. Security Issues in Grid Computing:

Security challenges in a grid environment, as in [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 that 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.

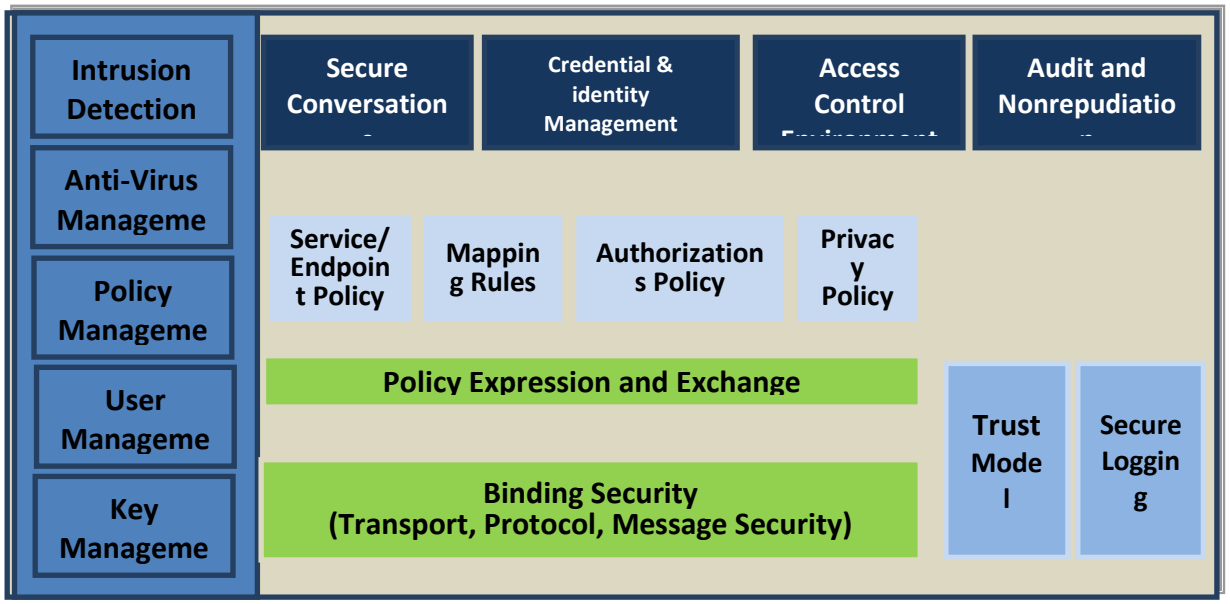

Fig.6 Grid security model

D. Security requirements:

Security requirements within the Grid environment are driven by the need to support dynamic, scalable, distributed virtual organizations (VOs), as in [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 gird computing systems have the vulnerabilities as under.

Type of grid computing system	Brief explanation	Most common vulnerabilities
Computational grid	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.	Programs with infinite loops can be used to bring down nodes of this grid, decreasing functionality
Data grid	Grid architecture responsible for storage and providing access to large volumes of data, often across several organizations	Users can overwrite data of other users if they exceed their available space-this corrupts the other users' data
Service grid	A grid which provides services that are not available on a single machine	Users can use the service grid to launch Denial of Service Attack (DOS) against another site

Table 1: Types of grid computing systems

To overcome these security issues, 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. The process of encryption converts the plaintext into encrypted form which is known as the cipher text and 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, as in [2].

Advance encryption standard 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, as in [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.

Rivest Cipher 4 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. 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.

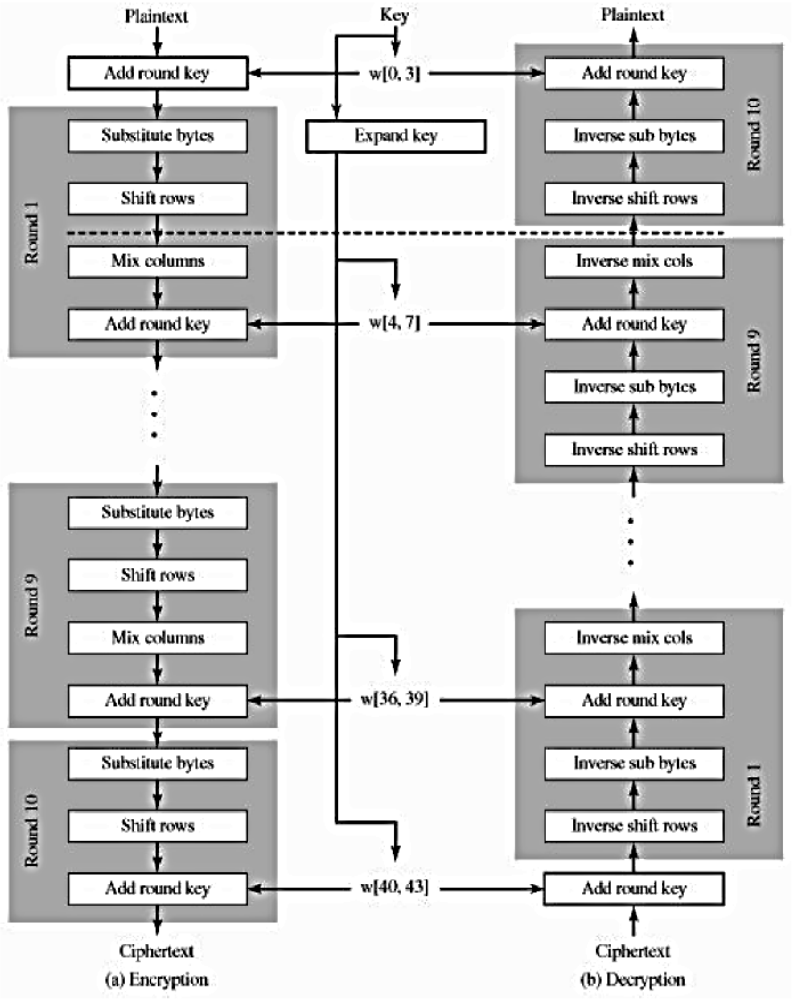

Fig. 7 Advance Encryption Standards

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. Review of Literature

As in [4]It provides overview of grid security services and other security solutions which are used in Grid middleware, Grid infrastructure and applications rely on the Grid middleware which provides common communication and messaging infrastructure for different resources and services exposed as Grid services, and also allows for uniform

security configuration at the service container or messaging level. This paper describe a set of research areas where prevalent Grid security solutions and architectures may no longer be able to provide a single consistent security architecture: provisioning of ensembles of resources across multiple domains for maintaining consistent life cycle management, user-controlled security domains, authorization session management and enforcement of policy where resource usage is subject to additional policy obligations that may be resource-specific and depend on the resource state, and the use of identity-based cryptography for dynamic security associations. By analysing several currently deployed Grid security systems and architectures in this paper we have attempted to indicate the limits of their applicability. Although by no means exhaustive in itself,

As in [5] explained that since late 1990s, Grid computing has become an increasingly important research topic within computer science. 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. We need new technical approaches to handle those security issues. During those years, many prominent companies and research institutes have proposed and implemented several architectures for grid and grid security. In this survey, first, authors introduce the Globus Toolkit, some commercial Grid productions and Grid Testbeds. Second it describes several Grid security architectures and research methods of security issues from research institutes and Universities. Next authors discuss the application of grid computing to the Global Information Grid (GIG). Finally we give some potential research topics.

Grid computing is a very vast research topic and security issue is very important in Grid. Several Grid architectures have been proposed in last ten years. The Grid systems have three security challenges: integration with existing system, interoperability with different environment and trust relationship among domains. Survey mainly focuses on interoperability challenge. Several research topics have been described, such as inter-Grid interoperability, policy express, access control for Web services and security Grid environment. Grid computing already has history for more than ten years. Although, many grid software services have been developed very well, for example, Resource management, resource discovery and fault tolerance, the research of Grid security just starts. Grid security still is one of the most crucial and difficult research topics. Based on the analysis to research of Grid computing in research institutes, Universities and industry

As in [7] explains that in the today world, security is required to transmit confidential information over the network. Security is also demanding in wide range of applications. Cryptographic algorithms play a vital role in providing the data security against malicious attacks. But on the other hand, they consume significant amount of computing resources like CPU time, memory, encryption time etc. Normally, symmetric key algorithms are used over asymmetric key algorithms as they are very fast in nature. Symmetric algorithms are classified as block cipher and stream ciphers algorithms. In this paper, authors compare the AES algorithm with different modes of operation (block cipher) and RC4 algorithm (stream cipher) in terms of CPU time, encryption time, memory utilization and throughput at different settings like variable key size and variable data packet size. The performance metrics were throughput, CPU process time, memory utilization, encryption and decryption time and key size variation. Experiments show that the RC4 is fast and energy efficient for encryption and decryption. Based on the analysis done as part of this research, RC4 is better than AES.

As in [8] explains that the increase use of computer and communication system by industry and organizations has increased the risk of theft of proprietary information. Although these threats require a variety of countermeasure, encryption process is a primary method of protecting valuable electronic information. The encryption process also needs to be dynamic in order to face new technique and more advance methods used by cryptanalysis. Substitution box (Sbox) is keystone of modern symmetric cryptosystem .They bring nonlinearity to cryptosystem and strengthen their cryptographic security. In this paper RC4 algorithm which is well known stream cipher is used to generate S-box for advance encryption standard (AES). The generated S-boxes are more dynamic and key dependant which will increase the complexity and also make the differential and linear cryptanalysis (DC&LC) more difficult. Various randomness tests are applied to the customized AES (AES-RC4) algorithm and the results shown that the new design pass all tests which proven its security.

As in [9] explains that during the procedure of resource discovery in Grid, a requester (consumer) may be offered several resources (providers) which identities have been verified to submit his task. How to make decision on selecting providers to complete his job reliably is an emergency. Establishing trust system is an alternative to respond the challenge. For the sake of future works in computational Grid are to refine the existing models, to define and to develop additional components, so define the trust model infrastructure for grid security module is necessity. This paper analyzes the fundamental trust requirements, proposes a trust signalling prototype and developments of simulating trust model which with we proposed computational model and signalling model for Grid security module is discussed at the end.

As in [11]this paper aims at developing a new hybrid cipher by combining the characteristics of two ciphers namely AES (Advanced Encryption Standard) and Rc4 (also known as ARC4). The characteristics of both the ciphers are studied and a new cipher combining the characteristics of both the ciphers is generated which is more secure than the original ciphers. AES characteristics are its security and its resistance against attacks and the major characteristic of Rc4 is its speed. Therefore these characteristics are imbibed in the newly generated cipher. Thus it proves to be faster than the original AES and secure against most attacks. Three combination techniques have been formulated to generate a hybridized cipher and the procedure along with the strengths and weaknesses outlined. The third cipher is the major cipher which is focused on in this paper. It is also shown that this cipher is resistant against most attacks. This will ensure the secrecy and confidentially of the messages it is used to encrypt.

As in [12] explained that adding digital intelligence and two-way functionalities to the power grid is one of the most flourishing topics in both academic and public institution communities. Efficiency, improved reliability and safety are the benefits promised by the new smart grid at the price of privacy and security challenges which are only in part similar to the security issues of IT networks. Authors survey the current grid architecture and the relation among the smart grid operators to analyze the security and privacy threats which needs to be addressed to secure the smart grid digital infrastructure.

III. 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.

IV. Research Methodology

1st Phase: This phase will contain the basic functionality and collection of information (basic grid applications). Layout for comparison has been done in this phase. In this phase we will use a simple scenario for grid network by comparing it with case study of grid example. Basic rivest cipher 4 will be implemented and will be used to combine with AES standard algorithm in latter part of the experimentation.

2th Phase: We will work on the proposed scheme to avoid the overhead provided by similar studies. 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. We will work on securecommunication by providing 128 bits AES encryption with RC4. Finally comparison of the base scenario with proposed scenario for finding the difference and fetching the information about energy consumption.

V. Conclusion

In research we will 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.

References

[1] Joshyhoseph and Craig fellenstein"Grid Computing"
[2] William stallings(2011) "Cryptography and Network Security" principles and practice 5th ed
[3] Introduction to grid computing with Globus, Luis Ferreira,Viktors Berstis,Jonathan Armstrong, Mike Kendzierski, Andreas Neukoetter, Masanobu Takagi, Richard Bing-Wo, Adeeb Amir, Ryo Murakawa, Olegario Hernandez, James Magowan, Norbert Bieberstein , IBM/redbook
[4] Yuri Demchenko, Cees de Laat Oscar Koeroo, David Groep "Re-thinking Grid Security Architecture" (2008) Fourth IEEE International Conference on eScience page 79-86
[5] Jianmin Zhu and Dr. Bhavani Thuraisingham," Secure Grid Computing", IJCSNS International Journal of Computer 216 Science and Network Security, pp.46-48, Vol.6, No.8B, August 2006.
[6] Jagdeep Singh, "Enhanced approach based on RC4 for securing grid", Master Dissertation Study, July 2012.

[7] Nidhi Singhal1, J.P.S.Raina,"Comparative Analysis of AES and RC4 Algorithms for Better Utilization," International Journal of Computer Trends and Technology, pp.177, Vol.2, July to Aug 2011.
[8] Abd-ElGhafar, A. Rohiem, A. Diaa, F. Mohammed,"Generation of AES Key Dependent S-Boxes using RC4 Algorithm", 13th International Conference on Aerospace Sciences & Aviation Technology, pp. 26 – 28, Vol.3, May 2009.
[9] Luo Zhen, Li Zhishu, Ca Biao,"A Trust Infrastructure for Grid Security Module", IEEE, Journal of Information Processing Systems, pp. 345-347, Vol.6, Issue.2, June 2010.
[10] Yilin Mo, Tiffany Hyun-Jin Kim, Kenneth Brancik, Dona Dickinson, Heejo Lee, Adrian Perrig, and Bruno Sinopoli,"Cyber–Physical Security of a Smart Grid Infrastructure", IEEE, Vol. 100, No. 1, January 2012.
[11] Prabhudesai Keval Ketan and Vijayarajan V, ''An Amalgam Approach using AES and RC4 Algorithms for Encryption and Decryption'', International Journal of Computer Applications, pp.12-17, Vol.54, No.12, September 2012.
[12] Alessandro Barenghi and Gerardo Pelosi,"Security and Privacy in Smart Grid Infrastructures ", 22nd IEEE International Workshop on Database and Expert Systems Applications, Vol.3, Issue.5, Sep 2011.
[13] Erin Cody, Raj Sharman, Raghav H. Rao, Shambhu Upadhyaya "Security in grid computing: A review and synthesis" Decision Support Systems 44 (2008) P.749–764
[14] http://www.adarshpatil.com/grid_tutorials.htm
[15] http://www.gridcafe.org/virtual-organizations.html
[16] http://www.buyya.com/
[17] http://www.ibm.com/developerworks/forums/forum.jspa?forumID=531
[18] http://www.cs.kent.edu/~farrell/grid06/lectures/index.html

