RSA Encryption Algorithm for Secured Grid Computing Data Transmissions

S.Ramya[1] Dr.T.Kokilavani[2]
[1]Research Scholar [2]Associate Professor
[1,2]Department of Computer Science
[1,2]St.Joseph's College, Truchirappalli-620002, India

Abstract— RSA encryption algorithm is a public key encryption technique and is considered as the most secure way of encryption and it is used for a long time. Our delicate data is placed in another infrastructure such as in the Grid Computing environment and the security worries increases with that. At that time, it is difficult to be guaranteed that our data is in the safe place. Thus, authentication has become the most important factor relating to this. There are many ways that has been discussed in the grid computing on the safe, efficient and scalable authentication that are either virtual centric or resource centric. Most of the grid computing uses public key infrastructure to secure the identification, but the exposure factor are still cannot be avoid. In order to satisfy the security need of grid computing environment, we design an alternative authentication mechanism using RSA encryption algorithm to secure the user identification.

Keywords: Encryption, Authentication, Information, Outsourcing, Secured

I. INTRODUCTION

Grid computing transmissions has been developing and emerging as a familiar platform for many consumers. Virtual organization in a grid generally gathers as well as incorporates computing and data resources from different organization for instance academic institution, scientific libraries and commercial companies. Thus, developing a reliable and competent access control mechanism for Grid is very much essential (Park & Chung, 2009). Most certificate authority (CA) in a regular public key cryptosystem (PKC) has to store vast amounts of public key certificates, real-time public key certificate has to be transmitted and stored in the signature checking process, which will raise unneeded waste of bandwidth and time delay. In inclusion, identity-based authentication protocol does not need to store large quantities of public key credentials, but key document becomes an inevitable problem, because the user's private key is generated by the key generation center. To overcome the aforesaid problem, Al-Riyami@etal.com [1] proposed certificate less public key cryptosystem (CL-PKC) in 2003. The Key generation center (KGC) generates the user's partial private key instead of generating the whole private keys.

II. LITERATURE REVIEW

There is Policy-based access control, in that Globus Toolkit (GT2) mechanism is utilized it is a resource management mechanism (JinWu, Leangsuksun, Rampure,& Hongong 2006). Boneh@etal.com [2] have proposed IBE from the Weil pairing which is comparably more secure and practical.

Gentry@etal.com [3] proposed a orderly signature schemes and IBC scheme. By default, authentication of users in the architecture of grid computing is using PKI certificates where flaws in the single point of Certificate Authentication (CA) server failure or compromise. Certificate management is a very complex and throws a poor scalability, which determines the number of sessions of protocol. GSI Li@et al.com [4]. Thus, the evolution of the usage of IBC/PKI in a grid computing architecture is done .

Lim@etal.com [5] In 2004 as an appropriate hierarchical IBC in grid environment. Other than that there are many access controls from previous researches such as Attribute-based access control (ABAC), where Identity Providers responsibility to giving the related attributes. As such they authenticate in the VO their members and create the attributions declaration consecutively to deliver the needed identity information to assist on making authorization decision given by the service and resource provider (Park & Chung, 2009). Mao@etal [6] introduced the Identity-based non-interactive authentication framework for grid computing where, this framework is a certificate-free and show significant performance improvement.

Rivest@etal.com [7] originally proposed the RSA algorithm construction at MIT 1978 conferences. One of the first practical public-key cryptosystems and is widely used for secure data transmission is RSA encryption. In this part, we describe the implementation of RSA authentication mechanisms in GridSim toolkit.

Zhang@etal.com [8] suffer from the public key replacement threat. Along with the design idea of little signature, we propose an authentication encryption mechanism that carries the characteristics of public key replacement threat resistance as well as high computational efficiency. The new encryption mechanisms give non-rejection and mutual authentication. In 2005, Lim H.W. and Robshaw introduce hybrid approach by combining PKI above the user level and IBC at the user level (Lim & Robshaw, 2005). This way of approach solves the key escrow, but loses non- interactive authentication and certificate-free way. In 2007 Chen, L. et al revisit grid security infrastructure (GSI) in the GT2 and improved the GSI architecture and protocol by proposing an alternative authentication framework Chen. The framework proposed by Chen, L., is still using certificate to do the work of authentication.

Zhang@etal.com [9] proposed identity-based signcryption scheme to meet cross-domain authentication. However, the architecture proposed and authentication mechanism is still not clear on how it to be implemented and the Certificate Authority (CA) are still not disappearing thoroughly. In this paper, we present our work on introducing RSA encryption authentication mechanisms to secured user identification.

Shamir@etal.com [10] introduced the concept of Identity based Cryptography (IBC) and given a signature scheme (Shamir, 1984).

III. GRIDSIM ARCHITECTURE AND COMPONENT

GridSim is made for a multilevel layer architecture for extendibility, as shown in Figure-1. This introduces new components or layers to be included and integrated into Grid Sim easily. In addition, the model of the Grid computing environment is captured by the layered GridSim architecture. Toolkit is based on SimJava2, a common purpose discrete-event simulation package implemented in Java framework. Therefore, At the bottom of the Figure-1 the first layer is operated by SimJava2 for handling the interaction or events among the GridSim components. Therefore, Handling the interaction or events among Gridsim component is managed by the first layer at the bottom Figure-1.

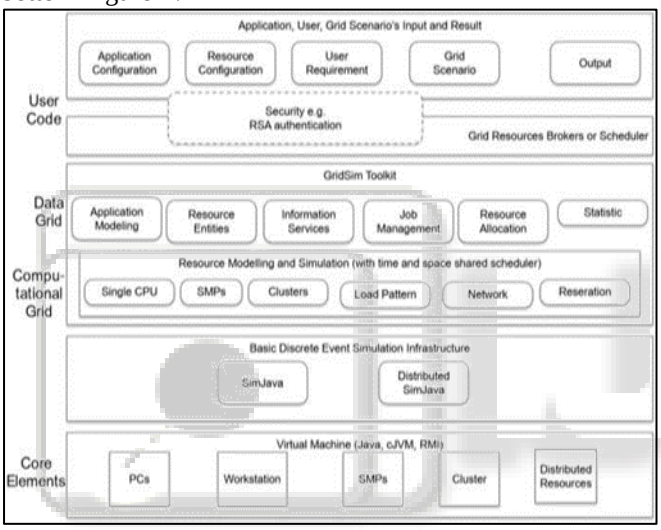

Fig. 1: Security Layers of GridSim Architecture

All the components in GridSim are working through the defined operations by SimJava for message-passing to communicate with each other. Grid resources such as network links, clusters and storage repositories which are namely the core elements of the distributed infrastructure models in the second layer. These core components are absolutely fundamental to create simulations in GridSim. The computational and data Grids are concerned with the modeling services and simulation of services at the third and fourth layers, respectively.

In case of the Data Grids, job management incorporates managing data transfers inbetween computational and memory resources. Replica catalogs, data services for files and data, are also especially implemented for Data Grids. The fifth layer holds components that help users in executing their own schedulers and resource brokers so that they can explore their own strategies and algorithms.

IV. OPERATIONAL METHODOLOGY

The following briefs an operational framework used in implementing this research. This is a set of procedures or methods used to conduct the research. The research strategy, design explains how the whole experimentation will be conducted is outlined. It is then followed by the detailed explanations of each phases involved in this research strategy. Each phase consists of outcomes that feed into the next phase of the research strategy. This part studies the current implementation of Grid Computing authentication. After that Grid Computing authentication framework development phase analysis for current practice of implementation is then conducted. In this phase, focused on authentication time for users to authentication server (e.g., broker, certificate authority (CA) and single-sign on server), communication time and computation time. A matrix will be developed to match or tailor between the security and performance of existing and current authentication framework.

1) Phase1: Reviewing current Grid Computing authentication framework implementation.

This part studies the current implementation of Grid Computing authentication. After that, Grid Computing authentication framework development phase analysis for current practice of implementation is then conducted. In this phase, focused on authentication time for users to authentication server (e.g., broker, certificate authority (CA) and single-sign on server), communication time and computation time. A matrix will be developed to match or tailor between the security and performance of existing and current authentication framework.

2) Phase2: Designing and implementing a prototype version of the RSA authentication framework.

On basis of the list of existing and present authentication framework mechanisms, the design and implementation of a new authentication framework is done. This phase will use a small set of data, such as users, routers, network and resources as an input for Gridsim simulator using Java program as an initial implementation.

3) Phase3: Evaluating an RSA encryption authentication framework using Gridsim toolkit.

The evaluation will used to compare the developed prototype authentication framework parameters to the existing and current authentication framework parameter. The Gridsim simulator using java programming is used to conduct a controlled Grid computing authentication framework in a stimulated environment.

V. PURPOSE OF GRIDSIM USED

There are several Grid simulators that provide various functionalities. Based on articulated that Bricks is designed for simulation of client server architectures in Grid computing (Klusacek, Matyska, & Rudová 2008 Klusáček & Rudová, 2010) The simulation and development of distributed applications in heterogeneous and distributed environment is done by the SimGrid. Evaluating and scheduling algorithms for MicroGrid and batch schedulers can be used for methodical study of the dynamic behavior of applications, middleware, resources, and networks are allowed by Simbatch. In this work, simulator is a Java based simulator toolkit. This toolkit is flexible and universal and it gives really good documentation. Functionality to simulate the basic Grid computing environment and its behavior is provided by the toolkit. Common entities are implemented simply and simulate simple jobs, network topology, data

storage and others useful functionalities are allowed by it and are given by GridSim.

VI. RSA AUTHENTICATION NETWORK ARCHITECTURE

In this part, we briefly describe RSA algorithm authentication mechanism network architecture. From the Figure-2 we can get that RSA authentication network architecture is composed of three entities, which are users, broker server and resources. The authentication is done, as depicted in Figure-2 where it's called asymmetric key cryptography because the key used for performing encryption and decryption are different and are normally referred to as public and private keys.

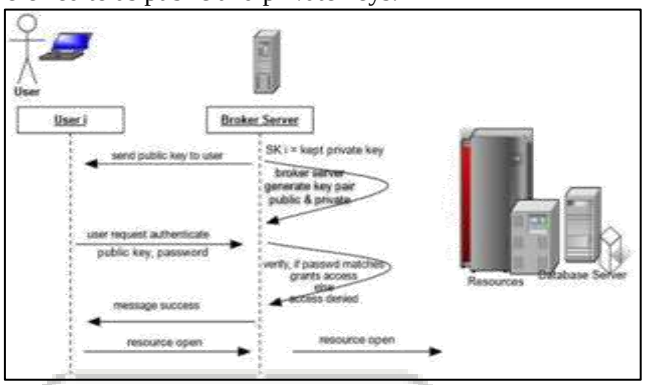

Fig. 2: RSA Authentication Mechanism

Initially, broker server generates pair key such as private and public key. The grid users gets the public key sent by the broker server and it retains the private key. The authentication process begins with a user authenticate to the broker server with password encrypted with the public key that corresponds to the pair key generated by broker server. Secondly, the broker server decrypted the user password and verifies the password. If the password matches, the broker server grants access to the network to use the resources. If not, access is denied.

VII. FINDINGS

The simulation experiment is done in GridSim, which is based on Java. Since SimJava is a discrete event simulation tool, and simulates various entities by multiple thread. This aligns well with the grid-computing environment. By reconfiguring these interfaces and connect the network link through two routers in the simulation environment special resources and users can be generated in the experiment.

The experiments were performed on Intel Core i72.9GHz machine with 8GB 1600MHz DDR3 RAM. The tests were run with different CPU ratings for a different number of available machines. The tests for 100 jobs with release dates, RSA authentication time, computation time, communication time and authentication time is performed. After running the simulations all the data are generated into log file in Java.

In this stimulation experiment we created where the total grid users are 5 to simulate the parallel request and uniformly distributed them among the two trust resources. Some of the parameters such as the maximum transfer unit (MTU) of a link and the latency are set same for all the network elements in the experiment.

Parameter	Value
Number of users	5
Number of resources	2
Number of gridlet	100
Baud rate	1000 bits/sec
Propagation delay	10 ms
MTU	1500 bytes

Fig. 3: Simulation Parameter

VIII. RESULT ANALYSIS AND SIMULATION

In this part, we analysis average RSA authentication performance and then simulation experiment gives precise result.

Authentication Cost

The execution of authenticated users from the user to the resources through broker server has been done. The figure-4 indicates that the result starts at 2.8 milliseconds and drop significantly to 1.5 milliseconds. This may be due to the fluctuation of the processor CPU time. After that the average of RSA authentication time is around 1.55 milliseconds per simulation time.

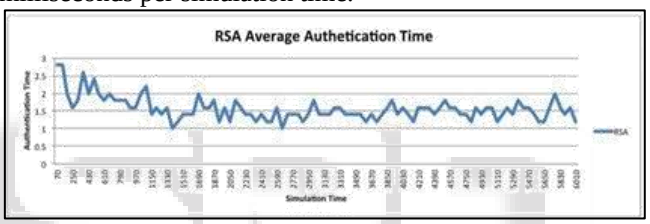

Fig. 4: Authentication cost vs Simulation time

Communication Cost

Based on Figure-5, it was found that average communication cost from the user to the resource would take around 4 millisecond over simulation time. We can see that the result shown in the simulation is significantly fast.

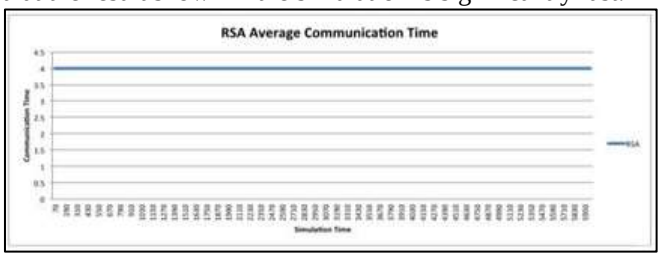

Fig. 5: Communication Cost vs Simulation time

Computation Cost

As a result, execution computation cost time; the average time for RSA computation time for task on each 5 users is shown in Figure-6. The graph illustrates the average computation time for RSA is approximately 25 milliseconds.

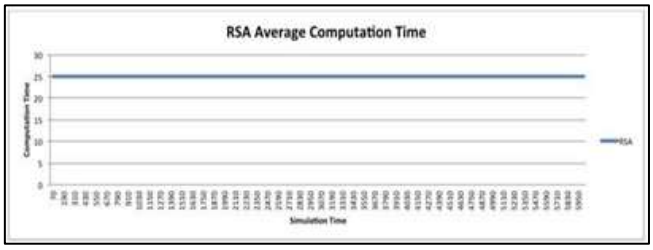

Fig. 6: Computation Cost vs Simulation time

IX. CONCLUSION

As we conclude, in this paper we are proposing a security in grid computing simulation to be implemented in authentication administration of grid computing environment as an extension to GridSim simulator. With this extension, GridSim has the ability to handle basic Grid security functionality. The most important point to implement this is the ability to control user management in a virtual organization (VO), whereas to protect the final manage of permission to share resources by the resource provider. In summation, we test the average communication time between users to resources through broker, computation time in the server and authentication time from server or broker. The result shown in this experiment are not very surprising, but the describe simulation was used as an example of the different functionality of the simulator. We hope this study can help solve problems arising in data grid computing security and help researcher make an important finding. In the future, we are contriving to look at the other authentication mechanism comparison with other crypto algorithm such as DSA, HMAC ECC and IBI in a control grid computing environment using the GridSim toolkit simulator.

REFERENCES

[1] Al-Riyami, S. S., & Paterson, K. G. (2003).Certificateless public key cryptography. In Advances in Cryptology-ASIACRYPT 2003 (pp. 452–473). Springer. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-40061-5_29.
[2] Boneh, D., & Franklin, M. (2001). Identity-Based Encryption from the Weil Pairing. In J. Kilian (Ed.), Advances in Cryptology — CRYPTO 2001 (Vol. 2139, pp. 213–229). Springer Berlin / Heidelberg. Retrieved from http://dx.doi.org/10.1007/3-540-44647-8_13.
[3] Gentry, C., & Silverberg, A. (2002). Hierarchical ID-Based Cryptography. In Advances in Cryptology — ASIACRYPT 2002 (pp. 149–155). Retrieved from http://dx.doi.org/10.1007/3- 540-361782_34.
[4] Li, H., & Sun, S. (2007). Identity-Based Cryptography for Grid. In Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on (Vol. 2).
[5] Lim, H. W., & Robshaw, M. J. B. (2004). On Identity-Based Cryptography and Grid Computing. In Computational Science - ICCS, 474–477.
[6] Mao, W. (2004a). An identity-based non-interactive authentication framework for computational grids. Technical Report HPL-2004-96. Hewlett-Packard Laboratories.
[7] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and publickey cryptosystems. Communications of the ACM, 21(2), 120–126.
[8] Zhang, J., & Mao, J. (2012). An efficient RSA-based certificateless signature scheme. Journal of Systems and Software, 85(3), 638–642. http://doi.org/10.1016/j.jss.2011.09.036
[9] Zhang, M., Yao, J., Wang, C., & Takagi, T. (2013). Public Key Replacement and Universal Forgery of SCLS Scheme. International Journal of Network Security, 15(1), 115–120.
[10] Shamir, A. (1984). Identity-Based Cryptosystems and Signature Schemes. In Advances in Cryptology, 47–53.

