Trends in Applied Sciences Research 7 (1): 78-86, 2012
ISSN 1819-3579 / DOI: 10.3923/tasr.2012.78.86


# A Dependable Model for Attaining Maximum Authentication Security Procedure in a Grid Based Environment

N.A. Azeez, A.P. Abidoye, K.K. Agbele and A.O. Adesina
Department of Computer Science, Faculty of Natural Science, University of the Western Cape, Private Bag X17, Bellville, 7535, South Africa

*Corresponding Author: N.A. Azeez, Department of Computer Science, Faculty of Natural Science, University of the Western Cape, Private Bag X17, Bellville, 7535, South Africa*

## ABSTRACT

Grid computing is an emergent computing innovation which offers endless access to computing infrastructure across various organizations (academia and industry). Since this technology allows aggregation of various computer systems for usage by different users to run applications, the information stored on it which may be sensitive and private, remains vulnerable. According to related research on the attribute based access control for grid computing there is no adequate and appropriate security mechanism to authorize and authenticate users before accessing information on a grid system. The issue of security in grid technology has not been fully addressed even though it is a precondition for optimizing grid usability. Having realized the paucity of security guarantees, this research work focuses on developing a model for securing data and applications deployed on a grid on the basis of double identity authentication and public key. The implementation of the model has undoubtedly guaranteed the security of sensitive information on a grid vis-α-vis strict adherence to security policies and protocols.

**Key words:** Grid, security, model, authentication, double authentication, encryption

## INTRODUCTION

Many authors have defined grid computing using several technical words and terminologies. According to Buyya (2002), the following definition was given.

The "Grid is a type of parallel and distributed system that enables the sharing, selection, and aggregation of resources distributed across multiple administrative domains based on their (resources) availability, capability, performance, cost and users' quality-of- service requirements." (Buyya, 2002).

Currently, Folderol, SETI@home and Distributed Net are projects that are currently exploiting (Wolfgang, 2000) various grid resources on the Internet. To ensure safety and security of resources within a grid system environment, there needs to be a set of policies for data access between the resource providers and resource consumers (Khider *et al*., 2010).

Public Key Infrastructure (PKI) is noted and recognized as a useful technology for securing a large scale network like grid. The main idea behind PKI is the certificate (Ali, 2002). The function of the certificate is to cement and bind (Price, 2003) the public key to a particular entity on the grid (Butler *et al*., 2000). The private key stands for the identity of an entity on the grid. PKI is well known for its interoperability (Ali, 2002).

One of the prominent models for implementing security on a grid is the Bell-LaPadula Model (BLM), also called the multi-level model which was formulated by the duo of Bell and LaPadula. This model is used for access control policy in both military and government applications (Zhao and Chadwick, 2008). With this security model, subjects and objects are grouped into different security rank and stage such that a subject can only access objects at a particular levels specified by his security level. In spite of the uniqueness of this model and its benefits, it only addresses confidentiality issues and its application is limited to systems where security levels do not change dynamically (Dallon *et al*., 2007).

Apart from the above approach, several other approaches (Goguen and Meseguer, 1982) have been employed to secure grid information to ensure adequate and efficient authentication (Gao *et al*., 2010) and authorization. Some of the prominent methods involved the adoption of traditional access control models such as Mandatory Access Control (MAC) model, Community Authorization Service (CAS) model, Discretionary Access Control (DAC) model and Role Based Access Control (RBAC) model (Ni *et al*., 2007).

Ali *et al*. (2009) has specified seven important security needs to protect grid information against attacks. These requirements are: authentication, authorization, availability, non-repudiation, data confidentiality, data integrity and privacy (Prasannakumari, 2009).

In an unsecured multi domain application environment like grid where various organizations interact with one another there bound to be some problems between the users and resources (Ni *et al*., 2007). We addressed some of these security challenges by adopting and implementing a double identity authentication scheme and public key system on a grid platform.

## BASIC CLASSES OF ENCRYPTION WITH TRADITIONAL CRYPTOGRAPHY

- **Product cryptography:** This is a process of combining various transformations such as modular arithmetic; substitution cipher and shift cipher together. The objective is to get a more reliable and secure (Zanjani *et al*., 2009) cipher than a single component to make it secure and resistant to cryptanalysis (Yanxiang *et al*., 2008)
- **Substitution cryptography:** The plaintexts are exchanged with some characters to produce ciphertext (Rasheed *et al*., 2010) base on a regular system. The formation of each of the characters can be changed but its position cannot be changed. The receiver performs an inverse substitution (Alfred *et al*., 1997) to decipher the text
- **Transportation ciphers:** The units of plaintext are rearranged in a unique and complex manner however the units remain unchanged (Yanxiang *et al*., 2008)
- **Shift cryptography:** This allows each of the characters to change its position without changing its formation in the plaintext. Matrix cryptography is an example of shift cryptography

### Definition of concepts:

- Authentication is any approach used to confirm that the identity is exactly the person who claims to be. This is always confirm with the aid of password and username
- Authorization is a technique of confirming if the person previously identified is permitted to have access to a particular resource or not

## APPRAISAL OF DATA ENCRYPTION TO ENSURE CONFIDENTIALITY

The purpose of data confidentiality is to protect data from being divulged to the wrong or an unintended party (Shen *et al*., 2006).

Two steps can be used to achieve data confidentiality (Hamid *et al*., 2009; Hoque and Avery, 2010) data encryption and data decryption. Also, two main types of cryptography can be used to provide data confidentiality (MSDN, 2005), they are: Symmetric and asymmetric.

**Symmetric cryptography:** In this type of cryptography both the sender and the recipient use a common key to carry out encryption and decryption (Fig. 1).

As illustrated in Fig. 1, symmetric encryption involves the following stages:

- The ciphertext message is created by the sender through the encryption of a plaintext with the assistance of a symmetric encryption algorithm as well as a shared key
- The ciphertext message is sent to the recipient by the sender
- The ciphertext message is decrypted back into a plaintext by the recipient
- Block cipher is the most popular of the symmetric-key encryption methods. Also, transposition ciphers and substitution ciphers are two prominent categories of block ciphers

**Asymmetric cryptography:** With asymmetric cryptography also called public key cryptography; different keys are used by the sender and recipient for encryption and decryption, respectively (MSDN, 2005). The sender encrypts data with one key and the recipient uses a different key to decrypt ciphertext (Fig. 2).

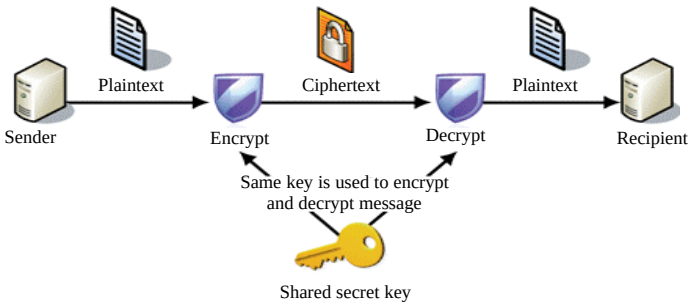


Fig. 1: The process of symmetric encryption

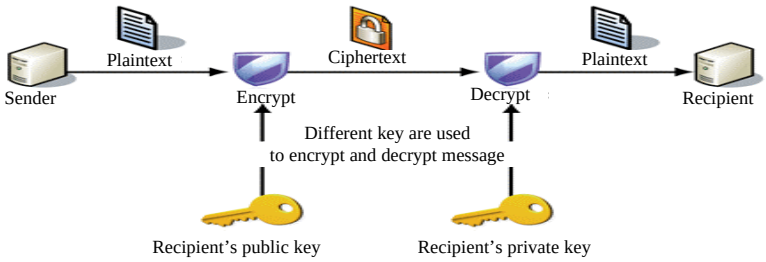


Fig. 2: The process of asymmetric encryption

As illustrated in Fig. 2, asymmetric encryption involves the following steps:

- The ciphertext message is created by the sender who encrypts the plaintext message with the aid of an encryption algorithm and the recipient's public key
- The ciphertext message is sent from the sender to the recipient
- The ciphertext message is decrypted back to plaintext with the aid of a private key that tallies with the public key that was used to encrypt the same message

## TRADITIONAL AUTHENTICATION APPROACH

To restrict and monitor the access of resources on a network (Rozyyev *et al*., 2011), user usually supplies and provides his identity (Ayofe and Oluwaseyifunmitan, 2009) based on recognition technology. The most common among the technology is password, Unique Identifier (ID) and token. The way in which this traditional technology is being employed is demonstrated (Fig. 3).

As the research in the area of computer and information security increases, the above technique of verifying user before accessing a network becomes unreliable and insufficient. This traditional approach has been confirmed and affirmed (Ayofe and Lawal, 2010) that they are very static and has not sufficiently satisfied the security demand in a data sharing environment. Due to this vulnerability, hacker takes the advantage to carry out malicious action on the grid (Ayofe and Oluwaseyifunmitan, 2009).

## THE CONCEPT OF RSA CRYPTO SYSTEM

Briefly, to implement Rivest, Shamir and Adleman (RSA) algorithm the following procedures are followed:

- Firstly, a random numbers p and q considered to be prime is selected and confirm that p! = q. Then the value of modulus with n = pq is determined before calculating phi, $\Phi = (p-1)(q-1)$
- Also, the public exponent e, $1<e<\Phi$ such that gcd (e, $\Phi$) = 1 is determined. Public key is taken to be {n, e} while private key is d

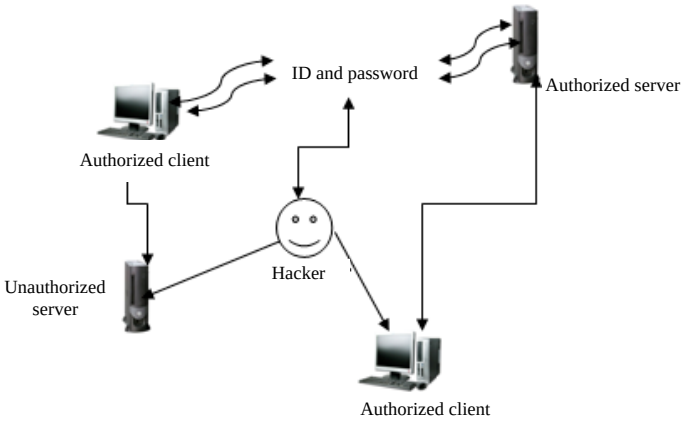


Fig. 3: Common traditional authentication approach

- Encryption is considered to be c = memod n while decryption is taken to be: m = cdmod n
- s = H (m) dmod n is taken as the digital signature while m' = semod n is for the verification
- If m' = H (m) signature is correct. It is believed that H is a publicly known hash function

## IMPLEMENTATION OF A SECURED MODEL IN A GRID BASED ENVIRONMENT

For the implementation of a secured model on a grid platform, the Fig. 4 serves as a dependable source of message information sharing.

Whenever, a user intends to establish a communication in a grid network, he supplies his flexible password and the required ID, respectively. The token code is evaluated by the server side thereby juxtapose it with flexible password supplied by the user. If it is confirmed and affirmed that the authentication is successful the server then comes up with a number as Token Session of a confirmed authentication. This is expected to be sent back to the client side.

When the client side confirms that authentication is succeeded by receiving token session information, the user will be prompted to enter the next flexible password which will have a binary value of 64-bit. At this stage, Hash algorithm (Dai *et al.*, 2009; Zhou *et al.*, 2008) is applied on the binary value to obtain 128-bit symmetric key. Handshake is therefore conducted between a client and the server. After the handshaking, the transmission of data encryption hereby commences. With the application of next flexible password, both the client and the server can successfully generate the secret key. With the double authentication procedure adopted in this model, it is sure and safe that hacker will not be able to carry out any malicious act that could be detrimental to the grid and its resources.

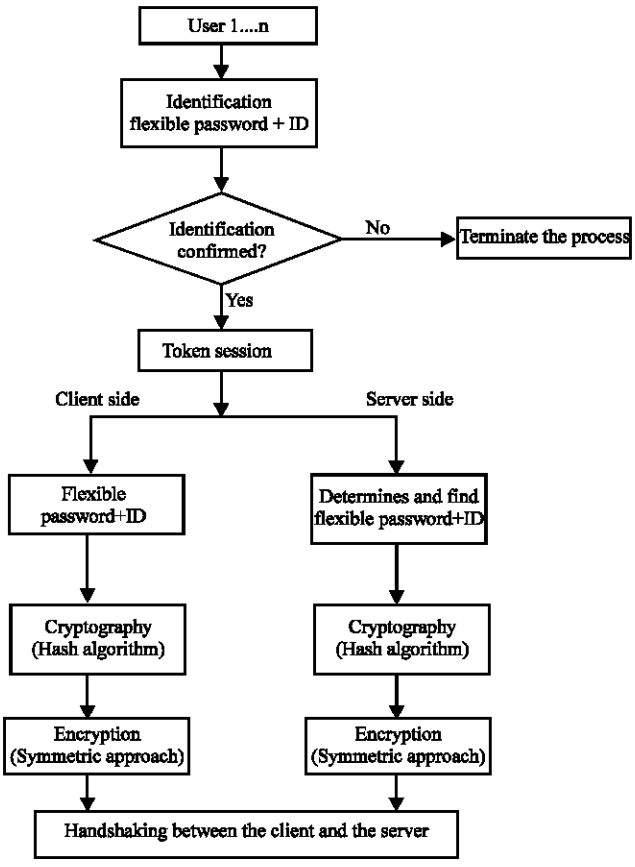


Fig. 4: Scenario of a dependable security model

Algorithm for the scenario is given as:

```
Start:
For GridUser = 1.... ...n
Enter ID: Submit (GridUser);
For User1..... .User n : identity NOT confirmed;
Terminate Action //Stop further action if the identity is not confirmed
Else
    Begin: Proceed Action
Token = Accepted (User);
Client (binary) = 64 bits
Hash algorithm (Calculate & determine) : Client (binary) =128 bits
Begin;
Handshaking (Client, server) //Communication is established between the server and the client
Then Begin Encryption; Obtain (client, server); secret key
Begin: Encryption
End
```

## PERFORMANCE EVALUATION WITH SIMULATION

To evaluate the performance of this double authentication scheme security model, a GridSim simulator was used. Two different graphs were obtained and the results of simulation are explained hereunder.

As shown in the Fig. 5, double authentication approach is flexible therefore resource each user can access varies with time according to the degree of authenticity of user. However, the degree of reliability of single authentication remains constant. This simulation result shows that with double authentication scheme, the rate of accessing any resource on the grid varies with time and directly depends on the authenticity of the user involved.

In Fig. 6, simulation result reveals that there is proportional increase in the turnaround time as the degree of authorization increases. But the average turn around remains constant at a point when a reliable and double authentication was not adopted.

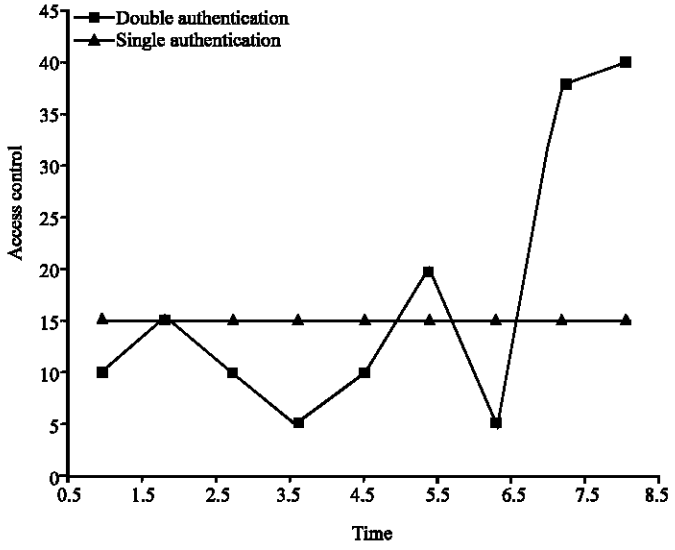


Fig. 5: Appraisal of double authentication scheme with respect to access control and time

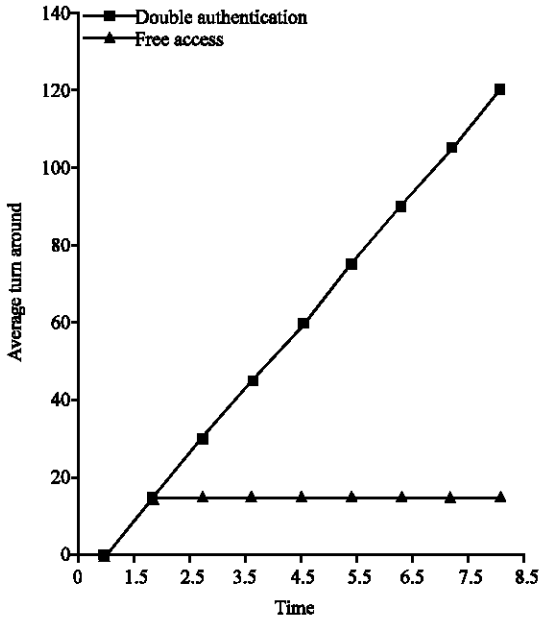


Fig. 6: Evaluation of average turn-around time with respect to time when applying double authentication

## CONCLUSION

Since security is an issue that is very crucial in a data sharing environment like grid, the proposition and implementation of a double identity authentication is a must to protect the integrity of resources across a multi administrative domains. This is mainly to achieve confidentiality, authentication, authorization and privacy on the grid network. It will be recalled that most of the approaches in the past have a lot of weaknesses which has rendered its significance to the lowest ebb. With the widespread and ubiquitous nature of grid computing vis a vis number of participants on the network the provision for a reliable authentication scheme could not be over emphasized. The implementation of the above authentication scheme has proved to be effective and useful in any grid based resource sharing environment.

## REFERENCES

Alfred, J., C.V. Paul and A.V. Scott, 1997. Handbook of Applied Cryptography. Institute of Technology, CRC Press, Inc., Massachusetts.

Ali, A.B., Z. Hussein and S. Francois, 2009. Access Control Mechanism for Mobile Adhoc Network of Networks (MANoN). Software Technology Research Laboratory, De Montfort University, Leicester, UK.

Ali, N.H., 2002. Critical evaluation of current approaches to grid security. M.Sc. Thesis, Royal Hooloway, University London, UK.

Ayofe, A.N. and O. Oluwaseyifunmitan, 2009. Towards ameliorating cybercrime and cybersecurity. Int. J. Comput. Sci. Inform. Security, 3: 1-11.

Ayofe, A.N. and W.O. Lawal, 2010. Towards a secured digitized library: Challenge, solution and implementation. Asian J. Inf. Technol., 9: 286-291.

Butler, R., V. Welch, D. Engert, I. Foster and S. Tuecke *et al.*, 2000. A national-scale authentication infrastructure. Computer, 33: 60-66.

Buyya, R., 2002. Economic-based distributed resource management and scheduling for grid computing. Ph.D. Thesis, Monash University, Melbourne, Australia.

Dai, Z., Z. Li, B. Wang and Q. Tang, 2009. An energy-aware cluster-based routing protocol for wireless sensor and actor network. Inform. Technol. J., 8: 1044-1048.

Dallon, G., P. Massonet, J.F. Molderez, C. Ponsard and A. Arenas, 2007. An analysis of the Chinesewall pattern for guaranteeing confidentiality in grid-based virtual organisations. Proceedings of the 3rd International Conference on Security and Privacy in Communications Networks and the Workshops SecureComm, Sept. 17-21, Nice, France, pp: 217-222.

Gao, A., W. Wei and X. Xiao, 2010. Multiple hash sub-chains: Authentication for the hierarchical sensor networks. Inform. Technol. J., 9: 740-748.

Goguen, J.A. and J. Meseguer, 1982. Security policies and security models. Proceedings of IEEE Symposium on Security and Privacy, (SCP'82), IEEE Computer Society, USA., pp: 11-20.

Hamid, S.H.A., M.H.N.M. Nasir, W.Y. Ming and H. Hassan, 2009. Improving the performance of the authorization process of a credit card system using thread-level parallelism and singleton pattern. Res. J. Inform. Technol., 1: 30-40.

Hoque, M.T. and V.M. Avery, 2010. Novel strategies to speed-up query response. Res. J. Inform. Technol., 2: 11-20.

Khider, H., T. Osman and N. Sherkat, 2010. Attribute-based authorization for grid computing. Proceedings of the International Conference on Intelligent Systems, Modelling and Simulation, (ISMS'10), Washington, DC., USA., pp: 71-74.

MSDN, 2005. Data confidentiality. http://msdn.microsoft.com/en-us/library/ff650720.aspx

Ni, X., J. Luo and A. Song, 2007. A trust degree based access control for multi-domains in grid environment. Proceedings of the 11th International Conference on Computer Supported Cooperative Work in Design, April 26-28, Melbourne, Vic., pp: 864-869.

Prasannakumari, V., 2009. A robust tamper proof watermarking for data integrity in relational databases. Res. J. Inform. Technol., 1: 115-121.

Price, G., 2003. Public key infrastructure: Challenges and challengers. Current Development in E-Commerce, Lecture Notes, RHUL.

Rasheed, M.M., O. Ghazali and N.M. Norwawi, 2010. Server scanning worm detection by using intelligent failure connection algorithm. Res. J. Inform. Technol., 2: 228-234.

Rozyyev, A., H. Hasbullah and F. Subhan, 2011. Indoor child tracking in wireless sensor network using fuzzy logic technique. Res. J. Inform. Technol., 3: 81-92.

Shen, Z.D., F. Yan, W.Z. Qiang, X.P. Wu and H.G. Zhang, 2006. Grid system integrated with trusted computing platform. Proceeding of the 1st International Multi-Symposiums on Computer and Computational Sciences, June 20-24, Hanzhou, Zhejiang, pp: 619-625.

Wolfgang, G., 2000. DOT-COMing the GRID: Using Grids for Business. In: Grid Computing-GRID, Rajkumar, B. and B. Mark (Ed.). Springer, Bangalore, India, pp: 1-3.

Yanxiang, H., L. Fei and H. Wensheng, 2008. The design and implementation of security communication model in grid networks. Proceedings of the 2008 International Conference on Computer Science and Information Technology, (CCSIT'08), IEEE Computer Society Washington, DC, USA., pp: 421-424.

Zanjani, M.S., N. Sakhaee and H. Shahbaznezhad, 2009. Mechanisms of customer knowledge management in E-commerce websites. Res. J. Inform. Technol., 1: 86-93.

Zhao, G. and D.W. Chadwick, 2008. On the modeling of bell-lapadula security policies using RBAC. Proceedings of the 17th IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, June 23-25, IEEE, Rome, pp: 257-262.

Zhou, K., L. Meng, Z. Xu, G. Li and J. Hua, 2008. A dynamic clustering-based routing algorithm for wireless senor networks. Inform. Technol. J., 7: 694-697.