Secure Group Communication in Grid Environment

Dr Sudha Sadasivam G sudhasadhasivam@yahoo.com
Professor/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

Ruckmani V ruckmaniv@yahoo.com
PhD Research Scholar/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

Anitha Kumari K kesh_chse@yahoo.co.in
ME (SE) Student/Department of Computer Science
PSG College of Technology
Coimbatore – 641 004, India.

ABSTRACT

A Grid is a collection of resources that are available for an application to perform tasks. Grid resources are heterogeneous, geographically distributed and belong to different administrative domains. Hence security is a major concern in a grid system. Authentication, message integrity and confidentiality are the major concerns in grid security. Our proposed approach uses a authentication protocol in order to improve the authentication service in grid environment. Secure group communication is brought about by effective key distribution to authenticated users of the channels serviced by resources. The proposed approach facilitates reduced computation and efficient group communication. It also ensures efficient rekeying for each communication session. The security protocol has been implemented and tested using Globus middleware.

Keywords: authentication, grid computing, grid security, multicasting, encryption.

1. INTRODUCTION

Grid protocols and technologies are being adopted in academic, government, and industrial organizations. Grid computing facilitates remote access to high–end resources for computation and data intensive jobs. Researchers can access heterogeneous and geographically distributed hardware and software resources efficiently. Two important requirements in grid include the formation of virtual organizations (VO) dynamically and establishment of secure communication between the grid entities. A VO is a dynamic group of individuals, groups, or organizations that have common rules for resource sharing [1].

Security in computational grids encompasses authentication, authorization, non-repudiation, integrity, confidentiality and auditing. To avoid the illegal users from visiting the grid resources strong mutual authentication between grid entities should be guaranteed. Password-based authentication is extensively used because of its simplicity. Authorization allows a specific permission for a particular user on a specified resource (channels). Confidentiality of information in a VO should also be ensured [4]. The necessity for secure communication between grid entities has motivated the development of the Grid Security Infrastructure (GSI). GSI provides integrity, protection, confidentiality and authentication for sensitive information transferred over the network in addition to the facilities to securely traverse the distinct organizations that are part of collaboration [2]. Authentication is done by exchanging proxy credentials and authorization by mapping to a grid map file. Grid technologies have adopted the use of X.509 identity certificates to support user authentication. GSI is built on top of the Transport Layer Security (TLS) protocol. Both TLS and GSI operate at the transport layer. They require an ordered reliable transport connection, so typically they are implemented over Transmission Control Protocol (TCP). This approach is not suitable for web service-based technologies on the grid. Simple Object Access Protocol (SOAP) protocol [13] is used by the emerging Open Grid Service Architecture (OGSA). This necessitates for support message layer security using XML digital signature standard and the extensible markup language (XML) encryption standard [14]. Enhancements of SOAP messaging to provide message integrity and confidentiality are standardized in Organization for Advancement of Structured Information Standards (OASIS). The WS-secure conversation specification [15] describes how two entities can authenticate each other at the message layer. Grid middleware like Globus Toolkit™ Version 4.0, pyGridWare and Open Grid Services Infrastructure (OGSI).NET/Web Services Resource Framework (WSRF).NET (Wasson et al., 2004) use WS-secure conversation based on TLS authentication handshake in the SOAP message layer. Globus Toolkit [3] provides security services for authentication, authorization, management of user credentials and user information.

Wei Jiea et al. [5] have proposed a scalable GIS architecture for information management in a large scale Grid Virtual Organization (VO) with facilities to capture resource information for an administrative domain. The framework also incorporates security policies for authentication and authorization control of the GIS at both the site and the VO layers. Haibo Chena et al. [6] have applied trusted computing technologies in order to attain resource virtualization to ensure behavior conformity and platform virtualization for operating systems. Yuri Demchenko [7] has analyzed identity management in VOs and usage of Web Service (WS)-Federation and WS-Security standards. G. Laccetti and G. Schmid [8] have introduced a unified approach for access control of grid resources. (PKI) Public Key Infrastructure and (PMI) Privilege Management Infrastructure infrastructures were utilized at the grid layer after authentication and authorization procedures. Xukai Zoua et al. [9] have proposed an elegant Dual-Level Key Management (DLKM) mechanism using Access Control Polynomial (ACP) and one-way functions. The first level provided flexible and secure group communication whereas the second level offered hierarchical access control. Li Hongweia et al. [10] have proposed an identity-based authentication protocol for grid on the basis of the identity-based architecture for grid (IBAG) and corresponding encryption and signature schemes. Being certificate-free, the authentication protocol aligned well with the demands of grid computing. Yan Zhenga et al [11] use identity-based signature (IBS) scheme for grid authentication. Hai-yan Wanga. C and Ru-chuan Wanga [12] have proposed a grid authentication mechanism, which was on the basis of combined public key (CPK) employing elliptic curve cryptography (ECC).

Once the grid entities are authenticated, key distribution occurs between the grid entities to ensure secure communication. Some existing key distribution schemes include manual key distribution, hierarchal trees and secure lock. Manual key distribution lacks forward and backward secrecies, whereas hierarchical model requires more footprints. Secure lock method is computation intensive. The proposed system encrypts session keys thereby reducing computational costs, communication costs, and key storage footprint. Although the method is simple, it ensures good accuracy. The proposed work aims at authenticating the users and allocating channel resources to the users based on the availability of the resource and security weights. It ensures both user and resource authentication. Then encryption key to ensure secure communication among these members is distributed among the channel members. The message digest of the information to be transferred is encrypted for confidentiality using the key and then transferred to authenticated grid entities.

Reconcilable key management mechanism is proposed by Li [16] in which the key management middleware in grid can dynamically call the optimum rekeying algorithm and rekeying interval is based on the rates that the group members join and leave.

Li [18] proposed an authenticated encryption mechanism for group communication in term of the basic theories of threshold signature and basic characteristics of group communication in grid. In this mechanism, each member in the signing group can verify the identity of the signer, and the verifying group keeps only private key.

A scalable service scheme for secure group communication using digital signatures to provide integrity and source authentication is proposed by Li [17] . In this approach, Huffman binary tree is used to distribute keys in VO and complete binary tree is used to manage keys in administrative domain. Sudha [20] proposed to use tree-based approach for secure group key generation and establishment of communication among domains in a VO using trust relationships.

The proposed work aims at authenticating the users and allocating channel resources to the users based on the availability of the resource and security weights. Then encryption key to ensure secure communication among these members is distributed among the channel members. Digest of the information to be transferred is formed and then it is encrypted for confidentiality and then transferred to its peers. The remaining of the paper is organized as follows: Section 2 is constituted by the proposed authentication and channel distribution mechanism. Section 3 discusses about the analysis done so far. Section 4 discusses about implementation results and Section 5 concludes the paper.

2. PROPOSED SYSTEM ARCHITECTURE

The components of the system depicted in figure 1 are described as follows..
1) Registration component to register the legitimate users/managers of the channel.
2) Join/leave component to take care of authentication of the channel users.
3) Key generation system that generates the encryption key randomly.
4) Key distribution system that distributes the keys to the authenticated members of the channel.
5) Channel to distribute the encrypted information among the group members.

When legitimate entities (users and resources) register to the channel, the encrypted hash value of their passwords is stored in the authentication server. The proposed approach initially authenticates the user by matching its encrypted hash value with that stored in the authentication file. If authenticated, a random key is generated and distributed among the members in the channel or group. The message digest of the message to be transferred is encrypted and multicast to the group through the channel.. The receivers then decrypt and decode to get the original message (figure 2)

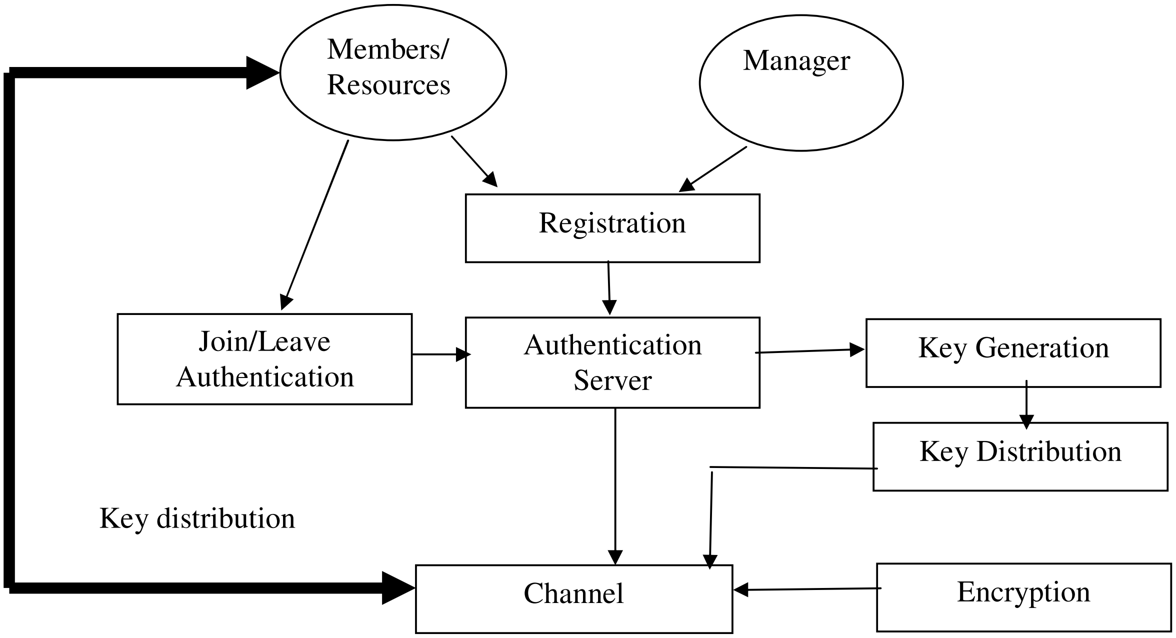

FIGURE 1: System Architecture

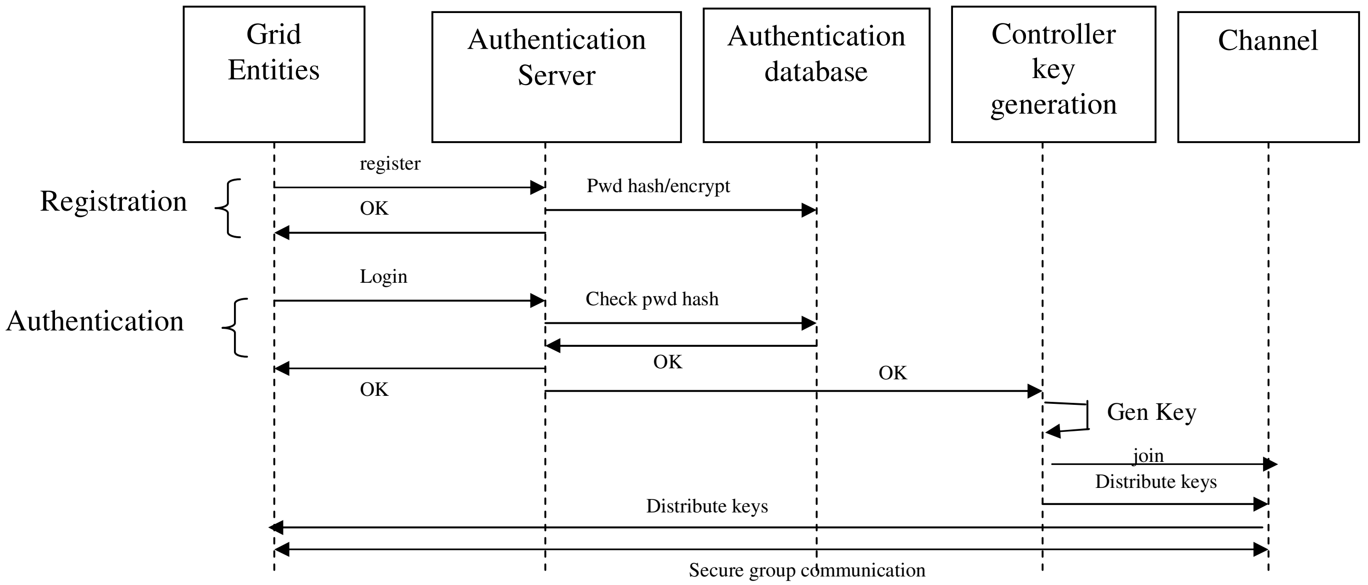

FIGURE 2: Process of secure group communication

The entire process consists of two major activities – authentication and key distribution for secure group communication. These activities are described in the following paragraphs.

2.1. Authentication Process:

The block diagram illustrating the registration process of the users is depicted in the Figure 3. Users who require services from the VO register using their username and password. The hash value of the password is calculated using Message Digest (MD5) algorithm and the encrypted password is stored in the authentication file.

The user who wants the services of VO has to login using the username and password. Here, u_i and pw_i refers to username and password of i^{th} user. The Authentication server calculates the hash value of the password and compares it with the decrypted value maintained in the authentication file. If the user is a valid user then the authentication server allows the user to join the channel and distributes the encryption key to the user.

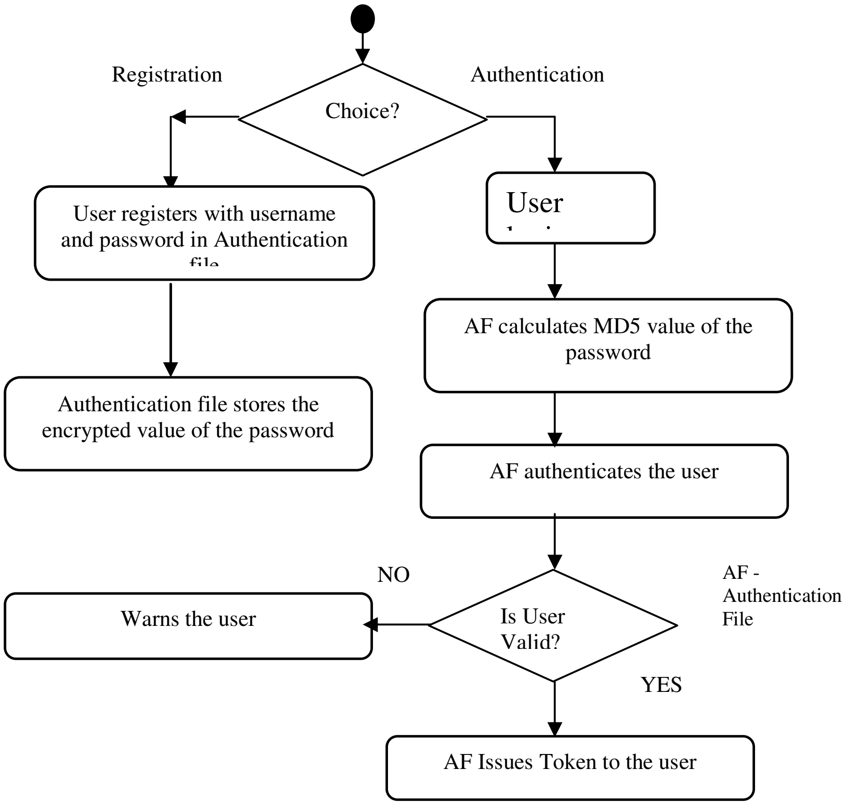
Registration
Authentication
Choice?
User registers with username and password in Authentication file
User
Authentication file stores the encrypted value of the password
AF calculates MD5 value of the password
AF authenticates the user
NO
Warns the user
Is User Valid?
AF - Authentication File
YES
AF Issues Token to the user

FIGURE 3: Authentication Scheme

2.2. Key Distribution And Secure Group Communication:

Confidentiality in information transfer in a distributed system is enabled by encrypting the information. Keys should be distributed securely among the members of the group. In existing approaches, each member shares a secret key with the group controller. If the information is to be transferred to ‘n’ members, ‘n’ encryptions followed by ‘n’ unicasts are needed. The computational complexity of the existing approach is overcome by using encoded session keys. Hence the proposed approach uses only an encoding followed by a multicast operation. This leads to reduced computation and provides efficient group communication. Further, the proposed approach ensures dynamic and secure group communication, forward secrecy and backward secrecy. The encoded key is used to manage member join, leave operations and for group communication. The security of the communication is achieved using one-way hash function to maintain integrity and encryption for confidentiality. Since a key is maintained for each channel/group, secure group communication is facilitated. The computation time of the key distribution is fast when compared to the key distribution by traditional algorithms like AES.

MD5 is used to generate the message digest. MD5 verifies data integrity by creating a 128-bit message digest from a message of arbitrary length. It can be used for digital signature applications, where a large file must be compressed in a secure manner before being encrypted using a public-key system. Steps in MD5 approach is listed as follows.

1) Arbitrary length message is padded with a '1' followed by '0's, so that its length is congruent to 448, modulo 512.
2) Then the length of the message (64 bits) is appended to it.
3) The MD5 algorithm uses four 32-bit state variables. They are initialized with constant values. These variables are sliced and diced to form the message digest.
4) 512-bit message blocks are used to modify the state in 4 rounds. Each round has 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Function F is different for each round. At the end of 4 rounds, the message digest is formed from the state variables. The message digest is then encrypted using Data Encryption Standard (DES) algorithm [19] and transmitted to its peer group member.

3. ANALYSIS

The analysis of the work has been done under the following heads:

3.1. Md5 Analysis:

The probability of two messages having the same message digest is on the order of 2^64 operations. The probability of coming up with any message having a given message digest is on the order of 2^128 operations. This ensures uniqueness of the message digest.

3.2. Replay attack:

Usually replay attack is called as 'man in the middle' attack. Adversary stays in between the user and the file and hacks the user credentials when the user contacts file. As key matching between the users is checked before file transfer and the information is encrypted before transfer, the probability of this attack is minimized.

3.3. Guessing attack:

Guessing attack is nothing but the adversaries just contacts the files by randomly guessed credentials. The effective possibility to overcome this attack is to choose the password by maximum possible characters, so that the probability of guessing the correct password can be reduced. As the proposed approach uses random generation of key, it is more difficult to guess the password.

3.4. Stolen-verifier attack:

Instead of storing the original password, the verifier of the password is stored. As the encrypted hash value of the password is stored, the proposed protocol is also more robust against the attack.

.

4. RESULTS AND DISCUSSIONS

The proposed authentication and distribution of channels has been implemented and tested on Globus middleware. It is tested with five valid and five invalid users. Each of the five valid users has their own username and password. Initially, they have created their user account using their username and password (Table 1). The authentication server stores the encrypted hash values of the passwords. As the hash values of the passwords are different, it ensures uniqueness.

Sl. No	Username	Password	Hash value
1	user1	admin	4c56ff4ce4aaf9573aa5dff913df913d
2	user2	Test2	Dfg45f4ce4aaf9573aa5dff913df913e
3	user3	test5	dddd6ffsdfdfdffffff913df997art567fg
4	user4	test8	4c56ff4ce4aaf9573aa5dff913df913d
5	user5	test10	sfggce4aaf9573aa5dff913df913fget

TABLE 1: Authentication File with unique hash value of passwords

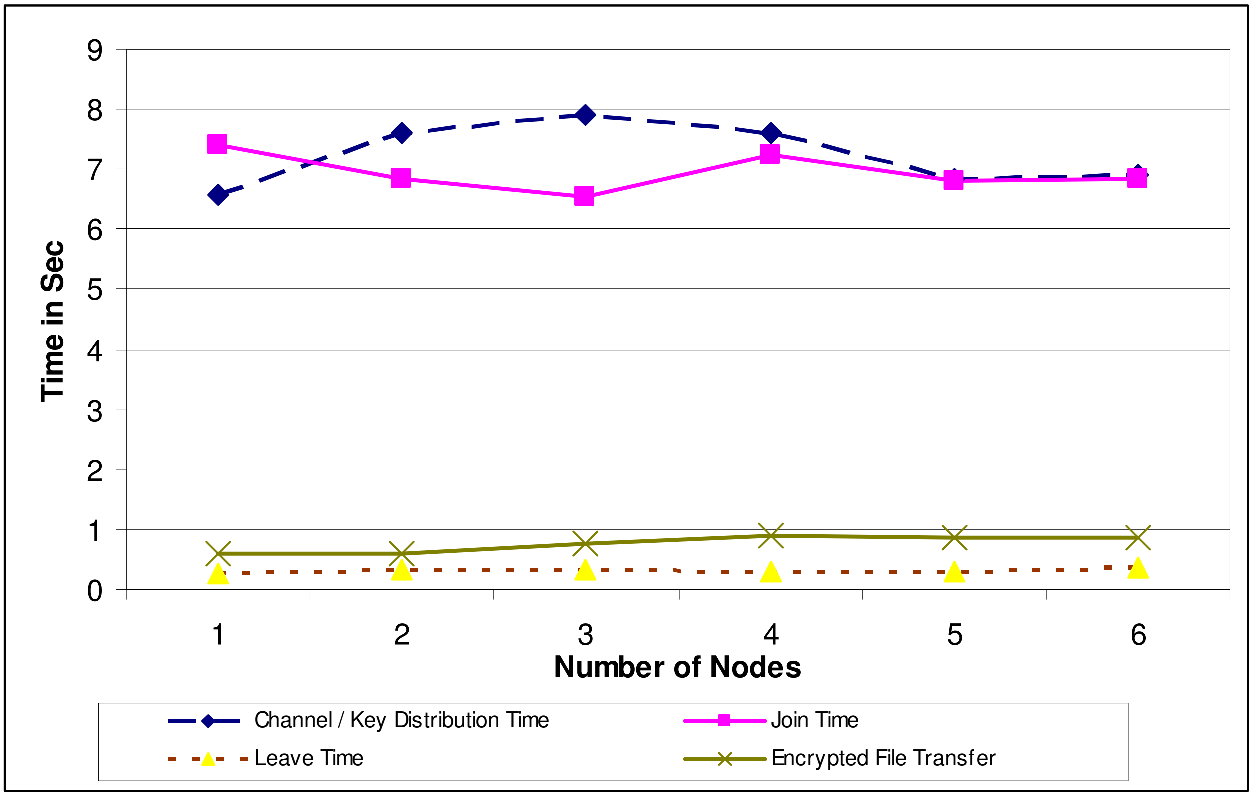

FIGURE 4: Experimental Results

Users join in the distributed channels across multiple machines in the grid. Once authenticated, key distribution and secure file transfer takes place. Figure 4 shows that the key distribution time and time for node join/leave remains almost a constant, irrespective of the number of nodes, incontrast to the hierarchical approach. Once the user joins the channel, secure file transfer occurs by encryption the information and multicasting it to the group members. Hence file transfer time also remains a constant in contrast to the unicast approach.

5. CONCLUSION

Grid Computing enables virtual organizations, to share geographically distributed resources. This paper proposes an effective approach for authentication and key distribution to ensure secure group communication in the grid environment. As the interpreted and distinct form of user credentials are maintained in the authentication files, there is very less chance to reveal the user credentials to the adversary. The implementation of our authentication protocol showed its effective performance in pinpointing the adversaries and paving the way to valid users to access resources in the VO by establishing as efficient computational channel distribution. Finally it is worth fit to host this scheme as a service in globus , also this basic scheme simply reduces computation complexity by replacing cryptographic encryption and decryption operations. Computation complexity further reduced by using algorithms like SHA , RIPEMD , IDEA .

6. REFERENCES

[1] Foster. I., Kesselman. C. and Tuecke. S, “The Anatomy of the Grid: Enabling Scalable Virtual Organizations”, International Journal of High Performance Computing Applications”, vol. 15, no.3, pp. 200-222, 2001.

[2] V.Vijayakumar and R.S.D.Wahida Banu, “Security for Resource Selection in Grid Computing Based On Trust and Reputation Responsiveness”, IJCSNS International Journal of Computer Science and Network Security, Vol.8, no.11, November 2008.

[3] I.Foster, “Globus Toolkit Version 4: Software for Service-Oriented Systems,” in the proceedings of the IFIP International Conference on Network and Parallel Computing, vol .1 ,pp. 11-33, 2004.

[4] Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman, Sam Meder, Laura Pearlman and Steven Tuecke, “Security for Grid Services”, in proceedings of the 12th IEEE International Symposium on High Performance Distributed Computing, pp.48- 57, June 2003.

[5]Wei Jiea,Wentong Caib, Lizhe Wangc and Rob Proctera, “A secure information service for monitoring large scale grids”,Parallel Computing, Vol.33, no. 7-8, pp. 572-591, August 2007.

[6]Haibo Chena, Jieyun Chenb, Wenbo Maoc and Fei Yand, "Daonity – Grid security from two levels of virtualization",Information Security Technical Report, Vol.12, no.3, pp. 123-138, 2007.

[7]Yuri Demchenko, “Virtual organizations in computer grids and identity management”, Information Security Technical Report, vol.9, no. 1,pp.59-76, January-March 2004.

[8]G. Laccetti and G. Schmid, "A framework model for grid security”, Future Generation Computer Systems, vol. 23, no. 5, pp.702-713,June 2007.

[9]Xukai Zoua, Yuan-Shun Dai and Xiang Rana, "Dual-Level Key Management for secure grid communication in dynamic and hierarchical groups", Future Generation Computer Systems,Vol. 23, no. 6,pp. 776-786,July 2007.

[10]Li Hongweia, Sun Shixina and Yang Haomiaoa, “Identity-based authentication protocol for grid”,Journal of Systems Engineering and Electronics, Vol. 19, no. 4,pp.860-865, August 2008.

[11]Yan Zhenga, Hai-yan Wanga and Ru-chuan Wang, "Grid authentication from identity-based cryptography without random oracles", The Journal of China Universities of Posts and Telecommunications, Vol.15,no. 4,pp.55-59, December 2008.

[12]Hai-yan Wanga. C and Ru-chuan Wanga,"CPK-based grid authentication: a step forward",The Journal of China Universities of Posts and Telecommunications, Vol.14, no. 1, pp.26-31, March 2007.

[13]Gudgin, M., Hadley, M., Mendelsohn, N., Moreau, J-J. and Nielsen, H.F. (2003) SOAP Version 1.2 Part 1: Messaging Framework. W3C Recommendation, Available at http://www.w3.org/TR/soap12-part1/ (accessed on June 2003).

[14] Eastlake, D. and Reagle, J. (Eds.) (2002) XML Encryption Syntax and Processing. W3C Recommendation, available at http://www.w3.org/TR/xmlenc-core/ (accessed on December 2002).

[15] Della-Libera, G. et al. (2002) Web Services Secure Conversation Language (WS-Secure Conversation). Version 1.0, available at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnglobspec/html/ws-secureconversation.asp (accessed on 2002).

[16] Li1, Y., Xu, X., Wan, J., Jin, H. and Han, Z. (2008) 'Aeolus: reconcilable key management mechanism for secure group communication in grid', 2008 IEEE Asia-Pacific Services Computing Conference.

[17] Li, Y., Jin, H., Zou, D., Chen, J. and Han, Z. (2007) 'A scalable service scheme for secure group communication in grid', 31st Annual International Computer Software and Applications Conference (COMPSAC 2007).

[18] Li, Y., Jin, H., Zou, D., Liu, S. and Han, Z. (2008) 'An authenticated encryption mechanism for secure group communication in grid', 2008 International Conference on Internet Computing in Science and Engineering.

[19] William M. Daley, Raymond G. Kammer,"DES", U.S. DEPARTMENT OF sCOMMERCE published in FIPS October 25, 1999.

[20] Sudha, G, Geetha J, "Secure communication between grid domains based on trust relationships and group keys", accepted in Int. J. Communication Networks and Distributed Systems, 2010.

[21] G Geethakumari, Dr Atul Negi, Dr V N Sastry ," RB-GDM: A Role-Based Grid Delegation Model", 2008 International Journal of Computer Science and Security (IJCSS) ,Volume :2 Issue: 1, Pages 61-72.