ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Security Model for Scady Grid Toolkit – Analysis and Implementation

Rakesh Bhatnagar[1], Dr. Jayesh Patel[2]

Asst. Professor, Dept. of MCA, S. K. Patel Institute of Management & Computer Studies, Gandhinagar, Gujarat, India[1]

Associate Professor, Acharya Motibhai Patel Institute of Computer Studies, Ganpat University, Kherva, Gujarat, India [2]

ABSTRACT: Security is the most critical aspect today in distributed computations. Grid computing shares and use resources in dynamic distributed environments. The dynamic nature of Grid environments results in security concerns in high performance applications. Almost all the communications in this distributed sharing environment are done using basic and standard cryptographic algorithms. But these algorithms do not provide the required security. Hence there is a need of new, strong and reliable technical approaches to solve these challenges.

This paper analyzes the GUI Grid toolkit – SCADY (Scady & Dynamic) which is designed by the authors, describes various security approaches and proposes the security mechanism for tasks of SCADY based on the X.509 certification so that high performance applications can be catered.

KEYWORDS: SCADY, X.509, Authentication, Delegation, Certificate

I. INTRODUCTION

Scady [1, 2, 3, 4] is built for the reason that the demand for the use of distributed resources and computing cycles are increasing day by day. Moreover, the power present in the networks (LANs) is not being utilized properly. Scady is based on Alchemi [8, 9, 10] Grid Toolkit which is becoming very popular for catering high performance applications in a grid environment. Grid systems, as are based on distributed resource sharing, uses standard security mechanisms such as authentication, access control, integrity, privacy, and no repudiation. Issues that are required to be taken care as listed in [5] are -

- Provision of authentication to verify the user's access
- Information of process which have user's computation and resources used by the processes to authenticate
- Provision to allow local access control mechanisms to be used without change
- Idea of number of nodes needed to complete the task
- Data sharing and Integritys
- Trust relationship policies
- Single sign on mechanism
- Capability for multiple implementations

To solve these issues, security mechanisms have to be designed to satisfy the above constraints. In this paper, we have discussed the various security implications and proposed the security mechanism using cryptography and certificate authentication for Scady toolkit using which high performance applications can be catered.

The Paper is organized as follows – Literature review is described in the next section. Section 3 highlights the security implications, Section 4 describes the proposed solution that removes the security issues, Section 5 describes the Conclusion, and Last Section contains the references.

II. LITERATURE REVIEW

We studied various Grid systems and their security mechanisms. The most popular system GLOBUS [11] uses three mechanisms - GSI (Grid Security Infrastructure)[11, 17], MyProxy & GSI-OpenSSH. GSI helps in providing APIs and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

tools for certificate management and authentication. MyProxy [11, 18] is open source software that manages X.509 security certificates and private keys through Public Key Infrastructure (PKI). GSI-OpenSSH [11, 19] is used to provide support to OpenSSH. It provides authentication and delegation in the way that login to the remote machine can be done without using password. For this it forwards X.509 proxy credential to the remote machine on login for authenticating the client.

UNICORE [12] uses X.509 version 3 certificates and single sign-on mechanism. X.509 certification mechanism is implemented through two steps in UNICORE. First, each client or server presents its certificate that contains public key and provides the private key to prove its identity. Second, private key is used to read the encrypted messages. An encrypted communication channel is established between different users on the Grid in this way. The certification mechanism uses the Secure Sockets Layer (SSL).

Alchemi [8, 9, 10] also works on X.509 certificate authentication. First, a trusted certified communication is set up between two nodes. Then the client node (Executor) is authenticated by the server node (Manager) through Certification and private keys. After authentication, Executor gets full delegation rights and access of applications provided by the framework.

HTCondor (High throughput computing Condor) [13], also uses X.509 Certificate authentication mechanism for security. HTCondor allows authentication of users and daemons, Encryption over the network and Integrity checking over the network. All Condor daemons in pool can share one certificate, or use one certificate per host. The Map file used transforms X.509 distinguished name into an identity.

Security challenges and future prospects are analyzed in [15] and security requirements according to the user behavior are reviewed from [16].

III. SECURITY IMPLICATIONS

Characteristics of Grid Environment as given in [5] can be summarized as –

- Dynamic and Large set of Users
- Dynamic and Large set of Resources
- Dynamic and Large set of Processes
- Communication Mechanism
- Authentication & Authorization Policies
- Credential Management

Issues of Security in Grid Systems are identified in the review findings and are summarized below -

- Improper Authentication management
- Improper authorization and access control policies
- Data sharing and Integrity violation
- Open communication protocols
- Weak trust relationship policies
- Inability of working with less resources
- Single sign on mechanism
- Proper credential management
- Interoperability with local security solutions
- Inter-domain Exportability
- Capability for multiple implementations
- Multiple security mechanisms
- Dynamic establishment of trust domains

Hence, there is a need of a strong and flexible security mechanism that can help in getting required security and functionality.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Proposed Solution

Security in SCADY is provided by using encryption and decryption algorithms and authentication by certification. RSA algorithm is used with SHA as cryptography method using 256 bit key or 512 bit key. For certification, X.509 certificates are used. Security Services [20] offered through the certificate are -

- Digital Signature
- Data Encipherment
- Key Encipherment
- Non-Repudiation
- Certificate Signing

For SCADY User certificate, the services used are: Digital Signature, Non Repudiation, Key Encipherment and Data Encipherment. For the Root Certificate, the service used is Certificate Signing.

Enhanced Key Usage Extension

Enhance key usage extension provided with X.509 certificate generation indicates the use of certificate's public key. It provides additional information such as whether the certificate is used for client authentication, server authentication, signing the document, IPSec Tunneling, time stamping, Code signing, SSL verification etc.

Additional information used in Scady through Enhanced Key Usage extension are -

- Secure Email - The certificate can be used for securing Emails.
- Client Authentication - The certificate can be used for authenticating the client.
- Server Authentication - The certificate can be used for authenticating the server.
- Document Signing - The certificate can be used to sign various documents.

We have created a root certificate as shown in Fig. 1 for the entire organization. Every certificate issued for a client will be signed by this Root Certificate. A Root Certificate (CA certificate) is used to digitally sign other certificates. In order to validate the certificates on other computers, the Root Certificate must be installed on the computers first.

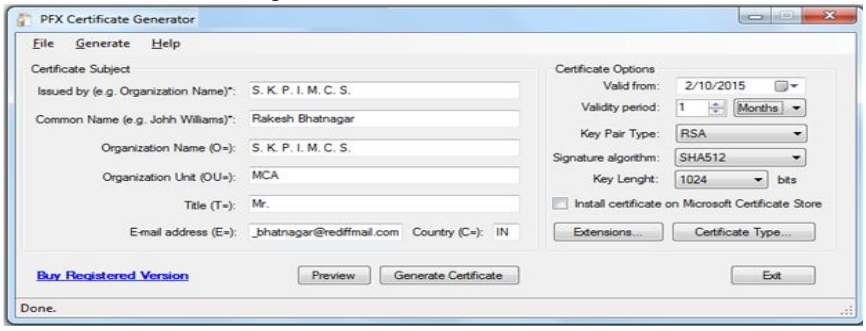

Fig. 1 Certificate Generator

Fig. 2 describes the type of certificate. The available types of certificates are – Standard Certificate, Self Signed Certificate and Certificate signed by Root Certificate.

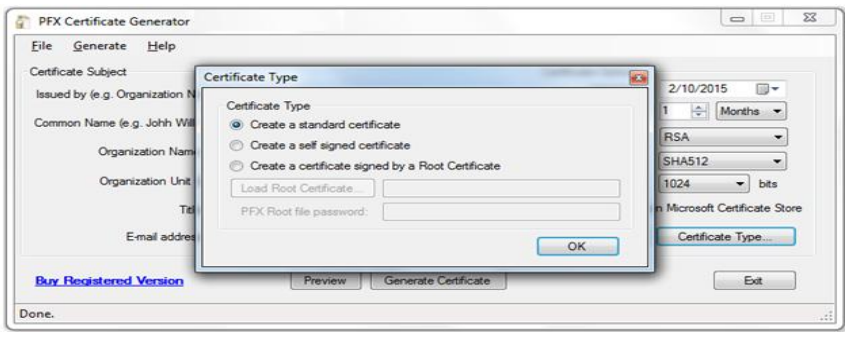

Fig. 2 Selecting the Type of Certificate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

Next we selected the extensions for the certificate as shown in Fig. 3. These extensions describe the key usage as well as the enhanced key usage of the certificate such as Secure Email, Client Authentication, Server Authentication, IPSEC User, IPSEC Tunnel etc.

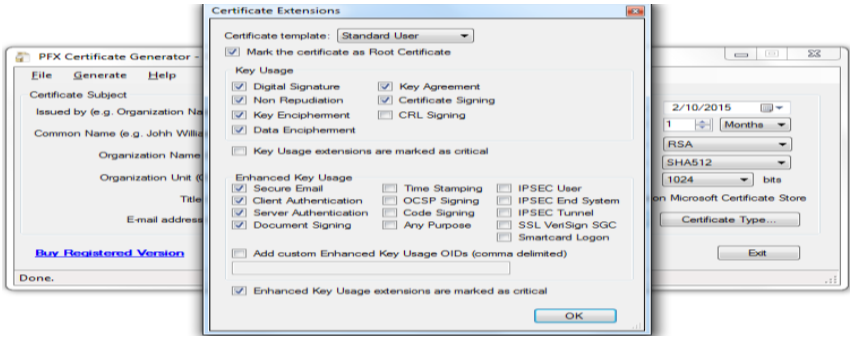

Fig. 3 Certificate Extensions

Finally the certificate will be created and will be ready to install for clients as shown in Fig. 4.

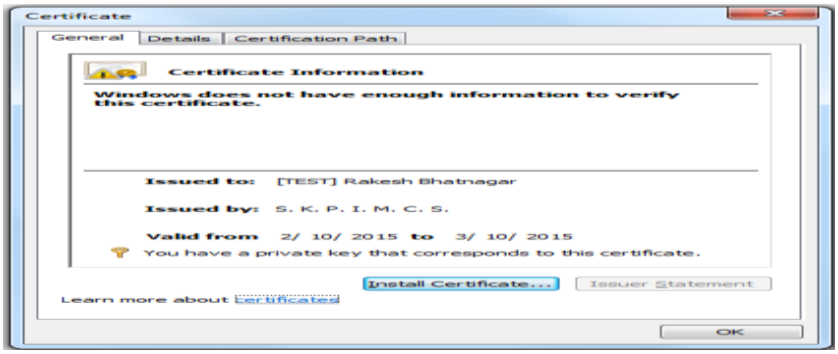

Fig. 4 Certificate Information

Issue of the Client Certificate Signed by the Root Certificate

In order to issue certificates signed by this Root Certificate, following steps are taken:

- "Standard User" Certificate is selected.
- Certificate Subject is filled with data like Issued to, Organization, E-mail address, etc.
- Root Certificate is then selected
- The present certificate is issued and saved.

For Client Certificates, 1024 bit key is used with RSA and for root certificate 2048 bit key is used. Fig-5, Fig. 6 and Fig. 7 describes how password is set for the certificate, and finally the certificate is generated successfully.

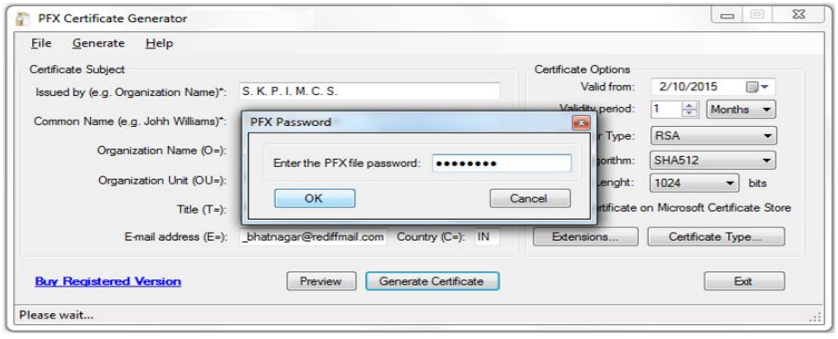

Fig. 5 Setting Password

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

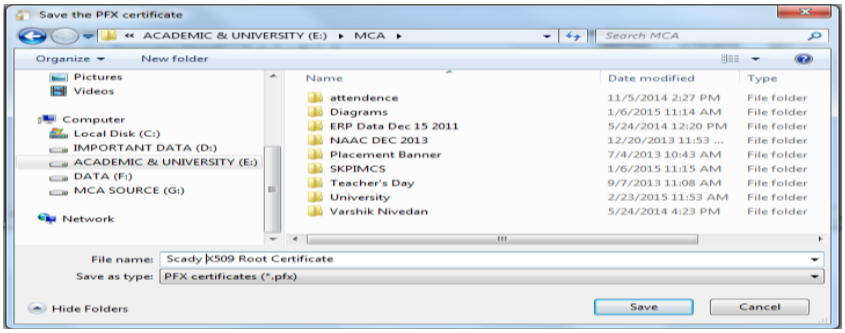

Fig. 6 Saving the Certificate

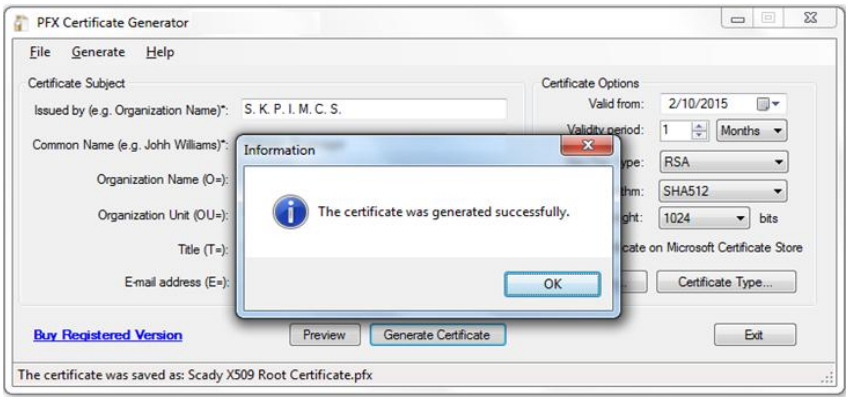

Fig. 7 Certificate Generator

After creating the certificates, they are issued as per the communication request. The proposed model given in Fig-8 is implemented and the application is tested. Initially, a root certificate is created with a validity of one month. The duration can be decided by the organization and as per the requirements of the application. The Proposed model using X.509 certificates throws the light on security model of SCADY.

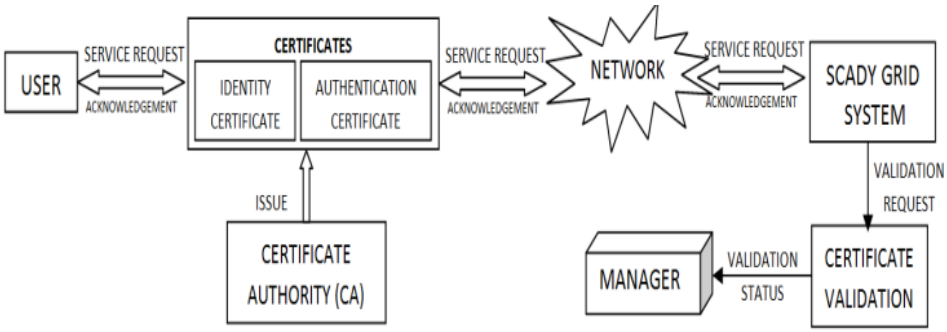

Fig. 8 Proposed Model

Use of these certificates and cryptography algorithms are represented through Use case Diagram as in Fig-9.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

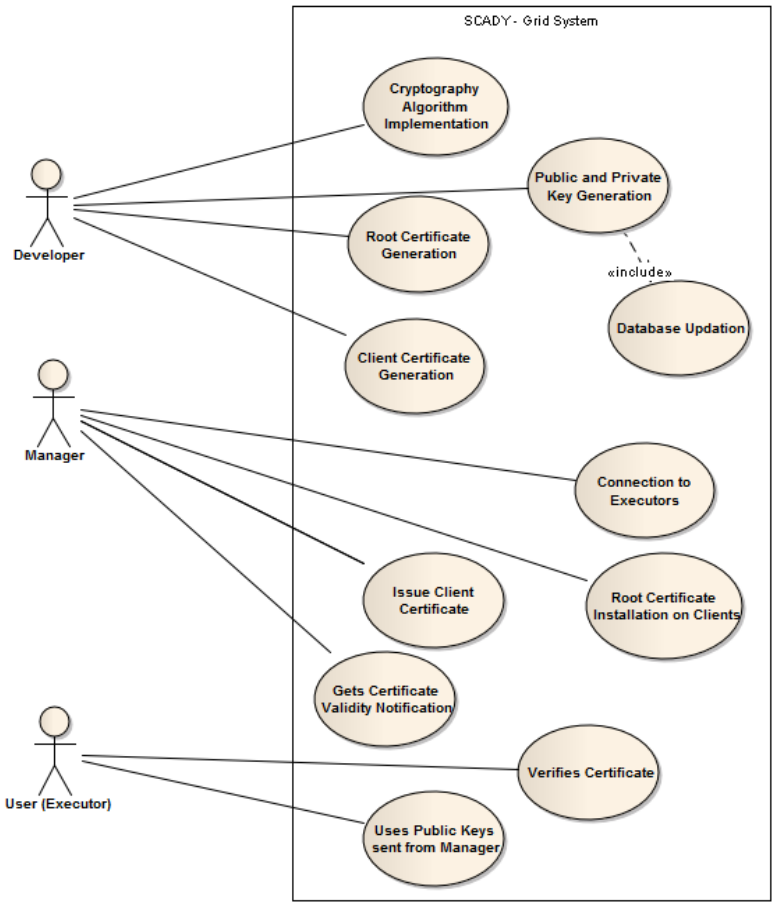

Fig. 9 Use Case Diagram

IV. CONCLUSION

In this paper, we studied Scady toolkit for Grid Computing. We found that even though, Scady is working fine in the grid environment, there was a need of security mechanism to secure and authenticate the communication. To remove this limitation, we proposed a security mechanism based on the review findings. The proposed model use X.509 certificate based delegation model and public key cryptography algorithms like RSA with SHA. Root certificate and client certificates are generated and issued.

We executed the grid toolkit with this certification model and found that the model is providing the required security to the system.

REFERENCES

1. Rakesh Bhatnagar, Dr. Jayesh Patel, Nirav Vasoya, "Implementation of Caching Algorithm in Scady Grid Framework", 6th IEEE International Conference on Computing Communications and Networking Technologies ICCCNT - 2015, July 13-15, 2015, Texas, USA.
2. Rakesh Bhatnagar, Dr. Jayesh Patel, Nirav Vasoya, " Dynamic Resource Allocation in SCADY Grid Toolkit", IEEE International Conference on Computing, Communication and Automation (ICCCA-2015), pp 724 – 728, 2015
3. Rakesh Bhatnagar, Dr. Jayesh Patel, " Scady: A Scalable & Dynamic Toolkit for Enhanced Performance in Grid Computing", IEEE International Conference on Pervasive Computing – ICPC 2015, Advances in Technology, pp 1 – 5, 2015
4. Rakesh Bhatnagar, Dr. Jayesh Patel, "API Specification for a Small Grid Middleware - SCADY", 11th IEEE India Conference – INDICON 2014, Emerging Trends and Innovation in Technology, pp 1 – 5, 2014

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 12, December 2015

5. R. Bhatnagar, Dr. J. Patel, "An Empirical study of Security issues in Grid Middleware", International Journal of Emerging Technology & Advanced Engineering , Volume 4 Issue 1, pp 470-474, 2014
6. Rakesh Bhatnagar, Dr. Jayesh Patel, "Performance Analysis of a Grid Monitoring System - Ganglia", International Journal of Emerging Technology & Advanced Engineering, Volume 3 Issue 8, pp 362-365, 2013
7. Rakesh Bhatnagar, Dr. Jayesh Patel, "Performance Analysis of a Grid Monitoring System - Autopilot", Journal of Sci-Tech Research (KSV – JSTR), Volume 4, Issue 2, pp 15 – 20, 2013
8. M. Bhardwaj, S. Singh & M. Singh, "Implementation of Single Sign-on and Delegation mechanism in Alchemi.Net based Grid Computing Framework", International Journal of Information Technology and Knowledge Management, Volume 4, No. 1, pp 289-292, 2011
9. Akshay Luther, Rajkumar Buyya, Rajiv Ranjan, and Srikumar Venugopal, "Alchemi: A .NET-based Enterprise Grid Computing System", Proc. of 6th International Conference on Internet Computing, ICOMP'05, June 2005.
10. Rajkumar Buyya, Akshay Luther, Rajiv Ranjan, and Srikumar Venugopal, "Alchemi: A .NET-based Grid Computing Framework and its integration into Global Grids", Technical Report, GRIDS-TR-2003-8, Grid Computing and Distributed Systems Laboratory, University of Melbourne, Australia, 2003
11. NV Kanaskar, U Topaloglu, C Bayrak, "Globus security model for grid environment", ACM SIGSOFT Software Engineering Notes, 2005 - dl.acm.org, Volume 30 Issue 6, pp 1 – 9, 2005
12. Unicore Client user manual retrieved Jan 10, 2014, from: *www.unicore.eu/documentation/manuals/unicore6/RichClient-.3.1.pdf*
13. J Frey, T Tannenbaum, M Livny, I Foster and S Tuecke, Condor-G: A computation management agent for multi-institutional grids, Cluster Computing, Springer, 2002
14. Marcos Dias de Assuncao, Krishna Nadiminti, Srikumar Venugopal, Tianchi Ma, Rajkumar Buyya, "An Integration of Global and Enterprise Grid Computing: Gridbus Broker and Xgrid Perspective", Grid and Cooperative Computing - GCC 2005, Springer, Volume 3795, pp 406-417, 2005
15. Maria Leitner, Stefanie Rinderle-Ma, "A systematic review on security in Process-Aware Information Systems – Constitution, challenges, and future directions", Elsevier, Information and Software Technology, Volume 56, Issue 3, pp 273–293, 2014
16. J Kołodziej, F Xhafa, "Meeting security and user behavior requirements in Grid scheduling", Simulation Modeling Practice and Theory, Elsevier, Volume 19, Issue 1, pp 213–226, 2011
17. GSI C – Globus Toolkit, https://dev.globus.org/wiki/GSI-OpenSSH
18. MyProxy Credential Management Service, http://grid.ncsa.illinois.edu/myproxy
19. GSI-OpenSSH Globus, https://dev.globus.org/wiki/GSI-OpenSSH
20. X.509 Certificate Generator Help Manual, http://www.signfiles.com/manuals/CertificateGeneratorUserManual.pdf
21. D. M Rathod, S. M Parikh and B.V Buddhadev, "Structural and behavioral modeling of RESTful web service interface using UML", Proc. of IEEE International Conference on Intelligent Systems and Signal Processing (ISSP), pp. 28-33, 2013
22. Aditya Patel, Pratik Thanawala, Dr. J G Pandya, "Grid Resource Brokering for High Performance Parallel Applications", International Journal of Emerging Technology & Advanced Engineering, Volume 3 Issue 4, pp 181-187, 2013
23. R. Nagaraja, Dr. G. T. Raju, "COMMPC - Component Based Middleware for Pervasive Computing", IJCSNS International Journal of Computer Science and Network Security, Volume 11 No.9, 2011
24. L. Ramakrishnan, "Securing Next-Generation Grids", IEEE IT Pro, March/April 2004.
25. WiMax Security 2014 [Online] http://www.topbits.com/wimax-security.html

BIOGRAPHY

Rakesh Bhatnagar is Asst. Prof. in the MCA Department, S. K. Patel College of Management & Computer Studies, Kadi Sarva Vidyalaya University, Gandhinagar, Gujarat, India. He has 13 years of teaching experience. He received M.Tech.(Computer Science) degree in 2006 and M.C.A. degree in 2002. Presently pursuing his research (Ph.D.), his research interest is in Grid Architecture, Middleware and Services.

Dr. Jayesh Patel is Associate Prof. in the MCA Department, Acharya Motibhai Patel Institute of Computer Studies, Ganpat University, Kherva, Gujarat, India. He has done MCA and received Doctorate degree in 2008. His research interest is in Grid Computing and ERP systems.