ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

Authorization Based Security Improvement in Grid Environment Using Facial Biometric

Gira Shantilal Patel

M.E. (I.T) (4th SEM), Information Technology, L.D. College of Engineering, Ahmedabad, India

girap.2010@gmail.com

ABSTRACT: Grid Computing means pools of distributed computer resources with multiple administrative domains. Grid computing over the internet requires more extensive security than within a single enterprises and robust authentication is employs in such a system security is the major issue related to and computing authentication is the important part in gird security. Other process in grid are depends on authentication. The aim of this proposed system is to enhance the security of the grid using facial bio metric. In this proposed system the study is done on existing grid security infrastructure. Simple user authentication using certificate has been selected as the reference for the enhanced authentication scheme. Here we have developed a system that uses a biometric input of user for authentication. We have use use's face as biometric input

Keyword: GridComputing, Golbus tool kit, GSI, GridFtp, MyProxyCredentials, Authentication, AuthorizationDelegation, Eigenspace Projection.

I. INTRODUCTION

This Paper aim to enhance the security based on authentication system in grid environment through facial bio metrics. Our Aim is to propose an authentication method which is based not only on the password and the user ID but also on the biometric input. To achieve aim of my proposed method, three major objectives have to be accomplished.

1) To analyse characteristics of Grid Computing environment, security challenges and issues in grid computing the existing password and certificate base authentication scheme, the existing Grid security infrastructure.
2) To analyse and design the facial bio metric authentication scheme that will secure the Grid Computing environment.
3) Integrate that facial bio metric scheme with Grid environment using Globus Tool Kit as a middle ware.

II. EXISTING AVAILABLE SECURITY IN GRID

A. Authentication

Authentication is usually linked close together with authorization. Authentication and authorization are often used in a combination in order to grant someone access to a service or a resource based upon a given identity. The authentication mechanism in a Grid is to provide plug points for the multiple authentication mechanism at hand and the means for conveying the specific mechanism used in the authentication operation [1].

B. Single Sign-On

Single sign-on is needed because in Grid multiple administrative domains are coordinate to reach the common goal. Doing authentication repeatedly in Grid is tedious process. In Single sign on should be able to authenticate once and have access to all resource of the Grid [1].

C. Credential Life Span & Renewal

Jobs on the Grid require security credentials through their run for accessing secure Grid resources. My proxy online credentials used for to generate credentials. Credentials have to be renewed after a given period of time [1].

D. Authorization

Authorization in Grid every local site wants to retain its authority on determining who can use its resource. In Globus Toolkit's GSI component authorization is done by "Grid Map file". The file contain mapping from a globally unique name assign to a grid user to a local account [1].

E. Delegation

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

To establishment of dynamic trust domains Delegation is require. Authority can be delegated from one entity to another. Delegation is also needed to secure dynamic service creation [8, 10]. Requestor can issue a special type of certificate signal by the original party that confirms that the holder of this certificate is allowed to act on its behalf. [1]

III. GRID SECURITY INFRASTRUCTURE

Grid Security Infrastructure (GSI) has been motivated by the need of secure communication between entities over the Grid. GSI provide integrity protection and confidentiality for sensitive information passed over the network as well as a mean of employing security mechanisms across different organizations. In this section we are going to summarize the characteristics of the GSI currently supported in GT4.0.

Basic security by GSI is public key cryptographic based on PKI. In PKI each entity is associated with a key pair. Data can be encrypted using any of the keys and decrypted with the other. Entities make publically available one of the keys which becomes the public key. The other key is securely and privately stored by the entity and is known as the private key [2]. By using the private key, the holder can encrypt messages and send them over a network. Such messages can be decrypted only with the holder public key.

If anyone decrypts the message using public key associated with an entity assume that no other entity could have seen that message. Public and private keys can be used for digitally signing of messages. Signed information assures the recipient that no tampering of the data occurred since its transmission. For signing data a hash value (a unique, small size identifier) is computed over the data intended for sending. The hash value is encrypted with the private key of the entity, attached and sent with the data on which the hash was computed. At the receiving part the hash value is re-computed over the received data (the algorithm for computing the hash value is known at both sides) and the signed hash received is decrypted with the sender public key. If the re-computed and the decrypted hash match than the data must be in the same form as it has been sent.

Private and public keys have to be bounded to a certain identity in order to identify the user or the service using them. For this matter PKI uses certificates. Certificates contain the following information: a distinguished name (DN) which uniquely identifies the entity holding the certificate, the public key belonging to the DN identified in the certificate, the DN of the Certificate Authority (CA) signing the certificate and thus attesting the relationship between the DN and the public key of the certificate, the CA digital signature and an expiration date. Important to observe is that a trusted CA is used to certify the pairing DN -public key in the certificate. The CA guarantees that the two belong together and signs the certificate so that it cannot be tampered. If the CA owns certificate is trusted then the user certificate can be trusted.

GSI uses certificates represented in X.509 End Entity Certificate format (check appendix B.1 for an example). X.509 End Entity Certificates can be obtained from a third party Certificate Authority (CA) or can be obtained from a “Simple CA” available with GT4.0 which can be installed for the local domain [1]. Authentication in GSI requires each party to trust the other part CA, and be able to prove the ownership of its certificate. Authentication of two parties starts with one party disclosing its certificate and being required to encrypt some random data generated by the second party. The encrypted data is decrypted at the second party (using the public key in the certificate already presented by the first party), and if it matches the initial data, authentication is achieved. The same process is repeated for having the second party authenticated as well [1].

The private key of a certificate is usually stored encrypted with a password, in a file residing on the local file system. This is done to prevent the use of the private key in case the file containing it is stolen (an unauthorized entity having the private key and the associated publically available certificate can easily impersonate the rightful holder of the certificate).

As we have seen the authentication process involves data encryption through the use of the private key. Each time authentication is required the user has to decrypt his private key by entering the protecting password. In a Grid environment, where a user program might access a large number of resources, typing this password each time access is attempted might not be a very comfortable approach, even more thinking that resources may be accessed at moments difficult to predict.

To solve this problem GSI make use of a delegation mechanism providing users with X.509 Proxy Certificates [22]. X.509 Proxy Certificates are short lived certificates generated with their associated private key by the user, and signed with his X.509 End Entity Certificate. If a proxy certificate private key is compromised, due to the certificate’s short lifetime (several hours) the harm that can be inferred is minimized. The proxy certificate private key can be protected only by local file system permission, in this

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

way user applications are able to use it whenever required without user input. If the proxy certificate expires, the user can generate a new proxy certificate with a new private key (it is possible to automotive this process so that long running jobs can work without user intervention). Proxy certificates are also used for delegating user rights to other agents/resources requiring contacting other resources on user behalf. The process is the same with the delegated part generating a proxy certificate (and keeping private the private key) and submitting it for signing to the delegating part. A proxy certificate can be signed by another proxy certificate (agents holding a delegated certificate may use it at their turn to delegate certificates to other agents on user's behalf) or an end entity certificate, with the process of authentication consisting of the pushing of the whole chain of certificates (having at root the user end entity certificate). The entire chain can be validated (by verifying with the public key of each certificate the signature on the next one in the chain - see below figure 1) and authentication achieved (provided if the user end entity certificate is signed by a trusted CA).

GT 4.0 delivers message protection through two mechanisms: transport level security (for transporting SOAP messages through secure channels) and message level security (by signing/encrypting parts of the SOAP messages).

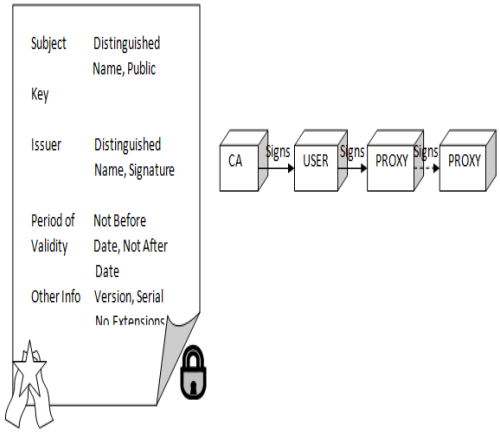

Fig 1. X.509 Certificate and Proxy Chain Certificate Validation

Transport level security is achieved by using X.509 certificates for authenticating parties and establishing a secure connection between the two over Transport Layer Security (TLS). Message level security is supported via the use of WS-Security standard or WS-Secure Conversation specification. If WS-Security is used in combination with X.509 certificates (proxy or end entity) protection of individual messages can be achieved by having parts of them signed or encrypted (the information is encrypted using the destination entity public key, and therefore, only the destination party is able to decrypt the data as it is the only one holding the private key).

For WS-Security a pre-existing context between the two entities is not required. If WS-Secure Conversation is used the keys of the two entities are used to establish a security context (containing a shared key which can be used for both encryption and decryption) allowing protection of messages with less overhead then using WS-Security.

A. **Authorization**

GT4.0 supports an Authorization Framework [25] for enforcing authorization on both client and service side. On the service side, authorization mechanisms rely on a configure chain of Policy Decision Points (PDPs) to determine if authorization should be granted or denied for a client invocation[3].

The framework supports user development and plugging of customable PDPs for service authorization. The decision regarding authorization is made base on the conjunction of all PDPs decisions that is authorization is granted only if all PDPs have returned a permit decision. PDPs logic can be implemented based on the client DN, the service accessed and the operation invoked.

Security descriptors are used for configure authentication and authorization mechanism. Such security descriptors can be defined at the container, service or resource (only for WSRF compliant services) level [3]. Clients can also use security descriptors for specifying how the accessed service should be authenticated and authorized.

Through the use of security descriptors, the container and each service can be configuring to use different credentials. Credentials can be either a proxy certificate or an end entity certificate and the associated private key. Authentication/encryption methods can be specified at service operation level. The available options are: GSISecureMessage and GSISecureConversation for message level security and GSITransport for transport level security. Messages can be protected for integrity (signed) or privacy (encrypted).

On the service side the authorization mechanisms available with GT4.0 rely on PDPs part of the distribution. These PDPs are configuring through the security descriptor of a service/container. The options are: self - identity of the service and client are expected to be the same, gridmap - the identity of the client must be mapped to a local user account

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

in a gridmap file, identity - a certain identity of the client is expected, host - a certain host name is expected of the entity requiring access, saml Callout - a SAML authorization callout to an external OGSA Authorization compliant service [26], userName - username and password based authorization (identity refers to the DN present in client certificate). On the client side the service authorization options are: self, host or identity.

IV. PROPOSED SYSTEM DESIGN & FACE RECOGNITION ALGORITHM

Here I have described my proposed system which is based on Authorization on Biometric input in Grid Environment. Figure 2 represent the whole scenario.

A. System Design

a. Steps

1. Install Globus Toolkit On more than One System. Consider one machine as a Server and remaining as Client machines.
2. At the Client Side design Login System which Capture the client's Face.
3. Send client's face image to the Server machine using GridFTP, this is making interface between System and Algorithm.
4. At Server side extracting client's face features and Compared with the Data based stored on the server machine. Feature extracting and comparison depend upon the particular technique deploy on the machine. Here we have used PCA based Technique for that purpose. Collect the result whether client is Authorized or not.
5. Send the result to the Client machine

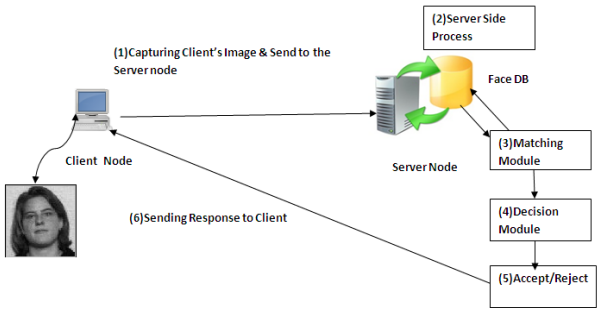

Fig 2 Proposed Systems

V. GRIDFTP

GridFTP provides a secure and reliable data transfer among grid nodes. The word GridFTP can refer to a protocol, a server, or a set of tools.

A. GridFTP protocol

GridFTP is a protocol intended to be used in all data transfers on the grid. It is based on FTP, but extends the standard protocol with facilities such as multi streamed transfer, auto-tuning, and Globus based security [4].

As the GridFTP protocol is still not completely defined, Globus Toolkit does not support the entire set of the protocol features currently presented. A set of GridFTP tools is distributed by Globus as additional packages. Globus Project has selected some features and extensions defined already in IETF RFCs and added a few additional features to meet requirements from current data grid projects.

GridFTP server and client

Globus Toolkit provides the GridFTP server and GridFTP client, which are implemented by the inftpd daemon and by the **globus-url-copy** command, respectively. They support most of the features defined on the GridFTP protocol.

The GridFTP server and client support two types of file transfer: standard and third-party. The standard file transfer is where a client sends the local file to the remote machine, which runs the FTP server. An overview is shown in Figure 3.

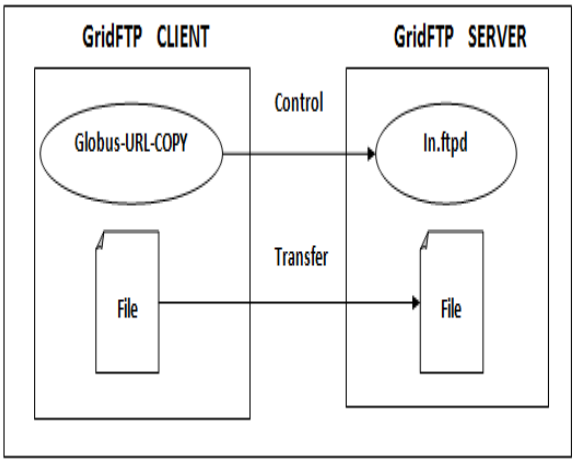

Fig 3.GridFtp Transfer

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

Third-party file transfer is where there is a large file in remote storage and the client wants to copy it to another remote server, as illustrated in Figure 3.

B. GridFTP tools

Globus Toolkit provides a set of tools to support GridFTP type of data transfers. The gsi-ncftp package is one of the tools used to communicate with the GridFTPServer. The GASS API package is also part of the GridFTP tools. It is used by the GRAM to transfer the output file from servers to clients [4].

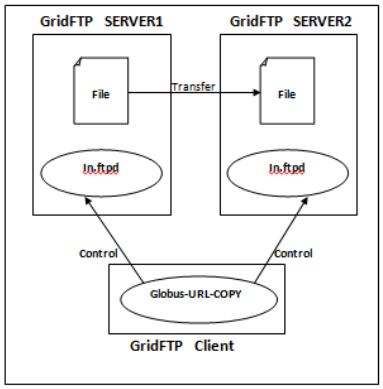

Fig 4 GridFtp Third Party Transfer

VI. FACE RECOGNITION ALGORITHM

1. **Centre data:** Each of the training images is cantered by subtracting the mean image from each of the training images [8, 9, and 10].
   $\mathbf{A^i = A^i - mn}$ **, where** $\mathbf{mn=1/P \sum_{i=1}^{P} A^i}$ **(1)**
2. **Create data matrix:** Once the training images are cantered, they are combined into a data matrix of size NxP, where P is the number of training images and each column is a single image as shown in equation
   $\mathbf{A= [A^{-1} | A^{-2}|.....|A^{-P}]}$ **(2)**
3. **Create covariance matrix:** The data matrix's transpose is multiplied by the data matrix to create a covariance matrix.
   $\mathbf{\Omega'=A^T A}$ **(3)**
4. **Compute the eigenvalues and eigenvectors of** O'**:** The eigenvalues and corresponding eigenvectors are computed for .

   $\mathbf{\Omega' V'=£' V'}$ **(4)**
5. **Compute the eigenvectors of** $\mathbf{AA^T}$**:** Multiply the data matrix by the eigenvectors.
   $\mathbf{V^{\wedge}=AV'}$ **(5)**

Divide the eigenvectors by their norm.
$\mathbf{v_i= V^{\wedge}_i/||v^{\wedge}_i||}$ **(6)**

6. **Order eigenvectors**

7. **Identify the Image using above technique:** Each test image is first mean cantered by subtracting the mean image, and is then projected into the same Eigen space defined by V.
   $\mathbf{B^i = B^i - mn}$ **, where** $\mathbf{mn=1/P \sum_{i=1}^{P} A^i}$ **(7)**
   And $\mathbf{B^{-i}=V^T B^{-i}}$ **(8)**

For recognition purpose here we have used Euclidean distance between eigenspace of train image and Euclidean distance of test image using equation (9)

$\mathbf{Distance= \sum_{i=1}^{P} (X_p - Y_p)^2}$ **(9)**

Here In this algorithm we have set One threshold value, If Euclidean distance is less than threshold value then Person is Unauthorized.

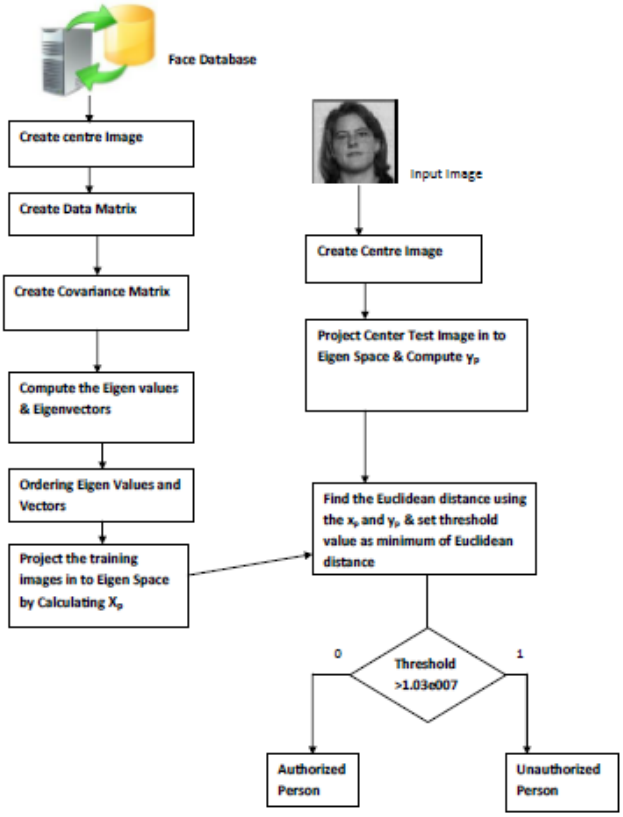

Fig 5 Face Recognition Algorithm

V. EXPERIMENT & RESULTS

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

A. **Experiments:**

Image Database

A face image database was created for the purpose of benchmarking the face recognition system. The image database is divided into two subsets, for separate training and testing purposes. During Our Experiment we have take 100 images were for training Database and 20 images are used as test images, Fig. 9 shows the training and testing image database constructed.

Figure (a)

Figure (b)

Fig.6 Training & testing image Database

Validation of Technique

The pre-processed greyscale images of size 80× 80 pixels are reshaped in MATLAB to form a 6400× 1 array with 6400 rows and 1 column for each image. This technique is performed on all 20 test images to form the input data for testing the recognition system. Then According to Algorithm Finding the Eigen Vectors and the Eigen Values of the images and Project the image in to Eigen space. Then normalize each image by dividing each pixel value by the norm of the image, so that the vector has a length of one. Then Find the xp for every image in the train Database.Simillarly For the test image do the above steps and find the yp.Then calculate the Euclidean distance between test image and train Database images using xp and yp.Then the image has Minimum Euclidian distance is the match image. For authorization purpose we have set one threshold value.

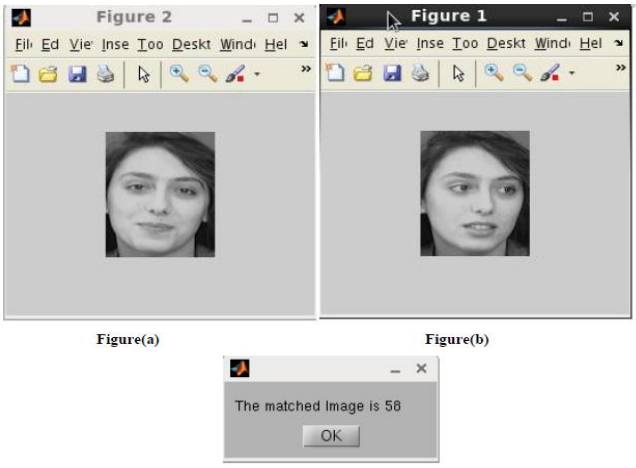

Fig.7 Result of Face Recognition System.

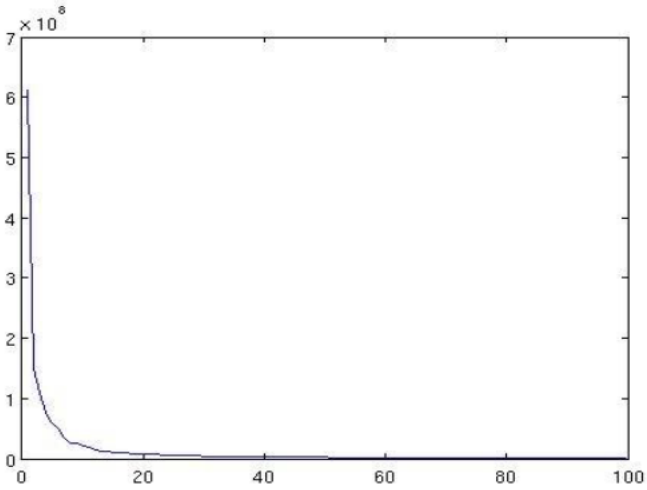

Fig 8 Eigen Values Vs Eigen Vectors

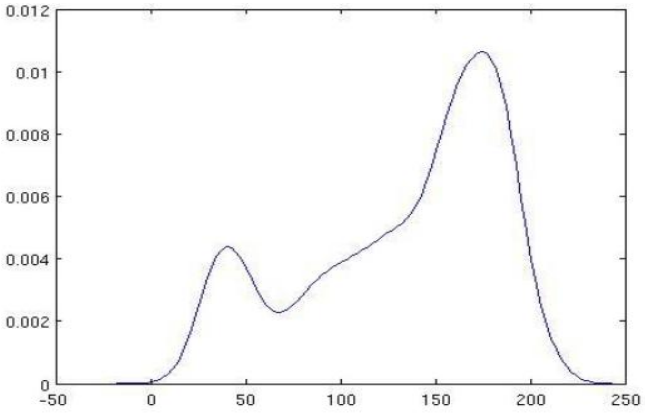

Fig 9 Euclidean Distance of Test Image

ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue 5, July 2012

B. **Result:**

Factors	**Proposed Authorization Scheme**	**General Authorization Scheme**
Computational Cost	High	Low
Mutual Authentication	Yes	Yes
Resistance to replay attack	Yes	No
Resistance to modification	Yes	No
Resistance to Man-in-the-middle attack	Yes	No
Factors in Authentication	4	2
Matching biometric data in remote server	Yes	No
Resist Id theft	Yes	No

Table I: Security comparisons of Proposed Authorization scheme with General Authorization scheme

VI. CONCLUSION

Extensive review and tests lead us to the conclusion that the GSI is suitable as a base Information Service infrastructure, due to its features like security, performance, extensibility, scalability and decentralized maintenance. In This report I have Interface GSI and Face recognition Algorithm by using Globus tool kit. I have used GridFTP protocol to transfer the image from the Client to server. My experiment shows that the technique can make more secure, potential and stronger Grid environment for well suited applications

ACKNOWLEDGMENT

I would like to express my gratitude to all those who gave me the possibility to complete this thesis. First, I thank my friend **Mr. Md.Salman R.Bombaywala, M.Tech, Assistant Professor, Department of EC, S.N.Patel Institute of Technology, Gujarat** as well as **Mr. Patel Rajiv C., Scientist, Advanced Numerical Research Analysis Group (ANURAG), DRDO, Hyderabad.** Without their guidance and patience, this dissertation would not be possible. I also wish to Record my thanks to Professors of the Department of Information Technology for their consistent encouragement and ideas.

REFERENCES

[1] Chakrabarti, A., Damodaran, A., Sengupta, S. Grid Computing Security: Taxonomy. IEEE Security & Privacy. IEEE computer society. 2007

[2] Ian Foster and Carl Kesselman. The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufman Publishers, 2nd edition, 2004.

[3] J.Basney, M. Humphrey and V. Welch. The Proxy Online Credential Repository. Software: Practice and Experience, 2005.

[4]Nataraj Nagaratnam, Philippe Janson, John Dayka "Security Architecture for Open Grid Services

[5] L. Pearlman, C. Kesselman, V. Welch, I. Foster, and S. Tuecke. The community authorization service: Status and future. In Proceedings of the Conference or Computing in High Energy and Nuclear Physics, La Jolla, California, USA, March 2003.

[6] Trucco E.and Verri A., Introductory Techniques for 3-D Computer Vision, New Jersey: Prentice-Hall, Inc.1998.

[7] Kirby M. (2000), Dimensionally of Reduction and Pattern Analysis: an empirical approach. Under contract with Wiley.

[8] Horn R.and Johnson C., Matrix Analysis, New York: Cambridge University Press, 1985.

[9] Turk M. A. and Pentland P. (1991) Face Recognition Using Eigen faces, Proc. Of IEEE Conference on Computer Vision and Pattern Recognition, 586-591.

[10] Nayar S., Nene S., and Murasr H. (1996), Real-Time 100 Object Recognition System. *Proceedings of* ARPA *Image Understanding* Workshop.

Biography

Gira Shantilal Patel Pursuing Master of Engineering in Information Technology at L.D.College of Engineering, Gujarat Technological University, Gujarat. She has received her Bachelor of Engineering Degree from Sarvjanik College of Engineering & Technology, Veer Narmad South Gujarat University, and Gujarat. Her research interest includes areas in Cloud Computing, Security and Virtualization.