International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 2, Issue 8 (August 2013), PP.28-33

Privacy and Authentication of Grid through Cryptography and Virtual Organization

Dr. S.P.Rasal
Mudhoji College Phaltan,Satara,Maharashtra, India

Abstract:- The data grid which is shared in different environment will not have the security challenges. The important hidden data(Such as banking) will reduces the data security in the environments. Here the different approaches that provide security as key sharing to prevent from unauthorized access of users. In this paper we present how the privacy and authentication of the grid through cryptographic system as encryption of the data and by the virtual organization it stores the data in form of fragments. The paper describes how the data can be secured in various organizations.

Index Terms*:-* Grid, Virtual Organization (VO), Cryptography.

I. INTRODUCTION

The main purpose of this project is to protect data in Grid Service. Which are faced while performing in data storage and we propose a cryptographic and fragmentation able to fulfill the storage security requirements related with a generic Data Grid scenario.

The Data Grid is a specific type of distributed system, where shared resources (processor or storage) are provided in a volunteer fashion by the participants. These environments potentially provide commodity resources not only for CPU-intensive tasks, but also for applications that require significant amounts of memory, disk space and network through put.

Data Grid depends on a set of widely distributed and un trusted storage nodes, therefore offering no guarantees about neither availability nor protection to the stored data. These security challenges must be carefully managed before fully deploying Data Grids in sensitive environments. We propose a cryptographic protocol able to fulfill the storage security requirements related with a generic Desktop Data Grid scenario, which were identified after applying an analysis framework extended from our previous research on the Data Grid's storage services.

One of the challenges for biomedical application is to provide efficient high-level interfaces, depending on the applications that enable access to Grids for non experts, ensuring transparent access to medical resources through services compatible with medical practice. As part of the interfaces, a flexible architecture for the management of the privacy of data is needed, compatible with medical practice and with preexisting Grid security systems are complex enough to be considered an obstacle in the successful Grid adoption.

The main objectives of the paper:

1) Cryptography method to prevent security of the data from unauthorized users.
2) To provide long term storage of the data which is in encrypted form.
3) Provides the access control mechanism for encryption of the data based on keys in VO.
4) It can be applicable to all the various environments.

II. EXISTING SYSTEM

One of the challenges for biomedical application is to provide efficient high-level interfaces, depending on the applications that enable access to Grids for non experts, ensuring transparent access to medical resources through services compatible with medical practice. As part of the interfaces, a flexible architecture for the management of the privacy of data is needed, compatible with medical practice and with preexisting Grid security systems are complex enough to be considered an obstacle in the successful Grid adoption. And also for the various organizations like government organization data in the existing system was not secure and there was no absolute protection guarantee for stored data.

III. PROPOSED SYSTEM

The main objective of this paper is to provide Grid middleware's such as TRENCADIS, with efficient and reliable privacy protection for sensitive data. This paper presents a model for long-term storage and management of encrypted data in distributed environments. Furthermore, the paper outlines how this model is implemented to preserve the privacy of patient information or any various secure information of different

organization in Grid-based collaborative computational infrastructures for biomedical applications. This paper delineates a dependable security framework in overextended to various organizations. Throughout the assembly of this framework, organizations will encounter different degrees of data integrity and confidentiality.

IV. VIRTUAL ORGANIZATION

A virtual organization (VO) [1] is formed from different real entities (e.g., medical centers, hospitals, governmental centers) , and probably also from different communities (e.g., physicians and researchers working in specific projects). Access to data is normally organized around VO membership.

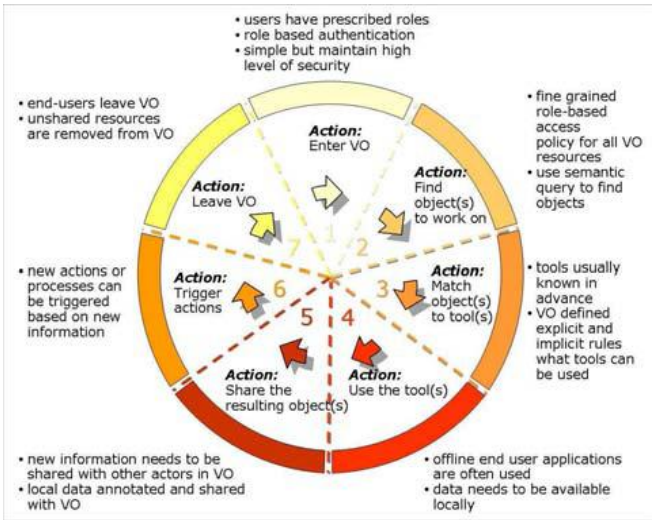


Figure 1: Generic virtual organisation end-user scenario actions.[2]

The developed use cases were abstracted into the generic virtual organization end user scenario presented in Fig. 1. Starting from available technologies, industry practices and trends, the project aim was to create knowledge, infrastructure and toolkits that allow a broad transition of the industry towards semantic, model based and ontology committed collaboration based on the grid technology (rather than the web, which is the infrastructure technology of the SWOP project [3]).

V. TYPICAL VO LIFE CYCLE PHASES

Virtual organization is fast becoming preferred organizational form for one-of settings to deliver one-of product and typically goes through four distinct lifecycle phases.

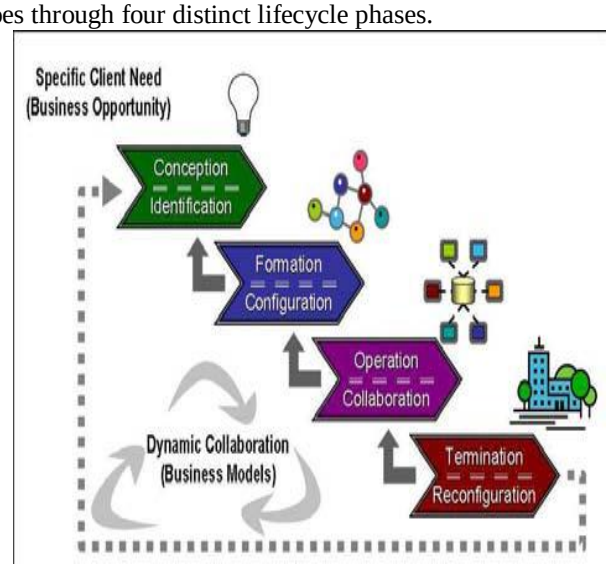


Figure 2: Typical virtual organization lifecycle [4].

Identification/conception typically begins upon a unique client need for a product/service that a single organization cannot deliver and serves as a business opportunity for a set of organizations which will combine competencies to deliver the product and/or service [4] that the client needs.

Formation/configuration focuses on the establishment of the VO in terms of role definitions, definition of information flow mechanisms, identification of information exchange formats, interoperability of inter-organizational tools, shared resource and services definition and configuration, etc.

Operation/collaboration is the main stage of a typical VO where different VO tasks are carried out in parallel and/or in series based on task needs.

Termination/reconfiguration. When a[4] VO consortium completes the delivery of the required product/service, it is terminated or reconfigured to form another VO (e.g. from a VO that develops a product to a VO that provides maintenance or service for that product).

VI. TRENCADIS ARCHITECTURE

Towards a Grid Environment for Processing and Sharing TRENCADIS is a Service Oriented Architecture (SOA) based in Grid Technologies, concretely in Open Grid Software Architecture [5] (OGSA). This architecture defines five layers, from the lowest to the highest abstraction levels from the point of view of the user. The components form the lowest layers (Infrastructure Layer), provide the functionalities (mainly share and process) through Grid Services. The components located in the upper layers (Application Layer) provide interfaces to the users through applications, which are developed on top of middleware components from the middleware Components Layer. All components communicate using the protocols provided by the Communication layer.

InTRENCADIS, the Key Sharing Service keeps the decryption key and provides to the authorized clients the data needed to decrypt objects in a secure way; and the EOUID Generator Service produces valid EOUID for new encrypted

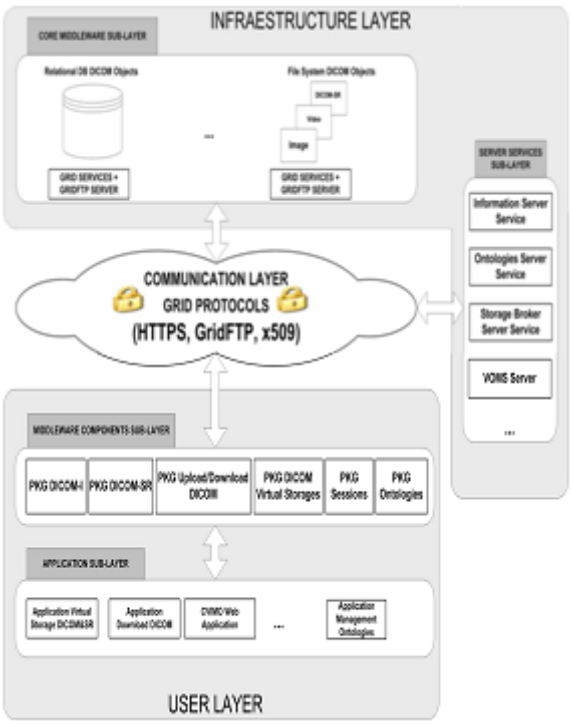


Figure 3: General view of TRENCADIS Architecture.

The security features of the system is followed[6]:

1) Authentication and Service Access.
2) Management of VOs. Grid users are organized into VO groups.
3) Data privacy may be preserved even when data are stored on a remote location

VII. ENCRYPTION AND DECRYPTION OF DATA

The model requires a public key cryptographic algorithm to encrypt and decrypt the information object, and 64-bit keys Data Encryption Standard (DES) [7] are used. Submitters of new/updated datasets utilize separate keys for each object. Encryption and decryption operations took place on the client, preventing the

overload of application servers running the IOS. Given that the risk of attacks is higher in servers that share multiple services (including public ones), and the impact could be higher since servers keep far more data than clients, keeping unencrypted information out of the IOS not only improves performance, but also helps to protect the information from unauthorized access from the Users.
Encrypted Object Unique Identifier (EOUID) that uniquely identifies the object in the Grid.

VIII. OPEN GRID SERVICES ARCHITECTURE

The Open Grid Services Architecture (OGSA) [8]describes an architecture for a service-oriented grid computing environment for business and scientific use, developed within the Global Grid Forum (GGF). OGSA is based on several other Web service technologies, notably WSDL and SOAP, [9]but it aims to be largely agnostic in relation to the transport-level handling of data.
Briefly, OGSA is a distributed interaction and computing architecture based around services, assuring interoperability on heterogeneous systems so that different types of resources can communicate and share information. OGSA has been described as a refinement of the emerging Web Services architecture, specifically designed to support Grid requirements. OGSA has been adopted as a grid architecture by a number of grid projects including the Globus Alliance. Conceptually, OGSA was first suggested in a seminal paper by Ian Foster called "The Physiology of the Grid", and later developed by GGF working groups which resulted in a GGF information document, entitled *The Open Grid Services Architecture, Version 1.5*. The Global Grid Forum continues to track Tier 1 use case scenarios used in the definition of the OGSA core services.

IX. FEATURES OF OGSA:

An architectural process in which the GGF's OGSA Working Group collects requirements and maintains a set of informational documents that describe the architecture.
A set of normative specifications and profiles that document the precise requirements for a conforming hardware or software component.
The OGSA Architecture [10]document describes an OGSA grid in terms of the following capabilities:

1) Infrastructure services.
2) Execution Management services.
3) Data services.

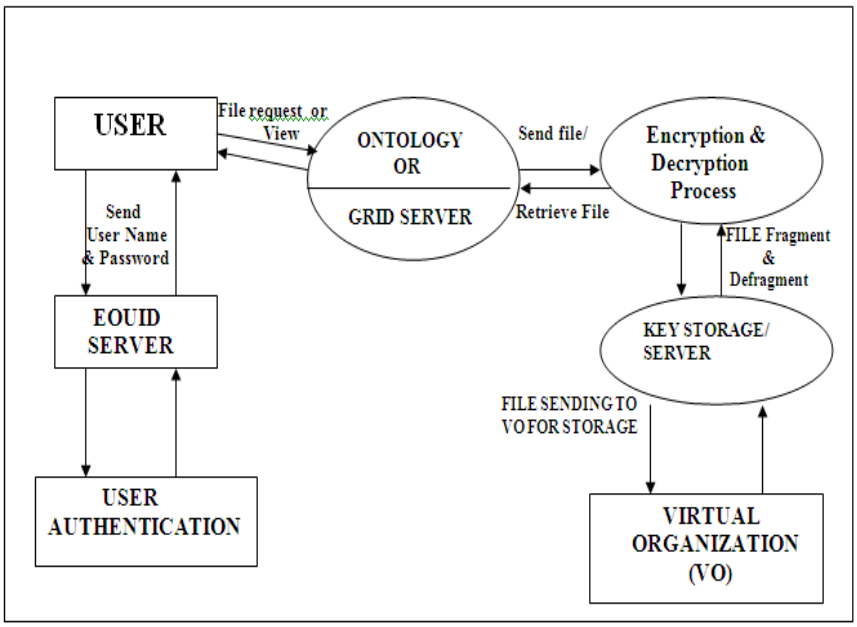


Fig 4: PROPESED SYSTEM ARCHITECTURE

VIRTUALORGANIZATION ARCHITECTURE:

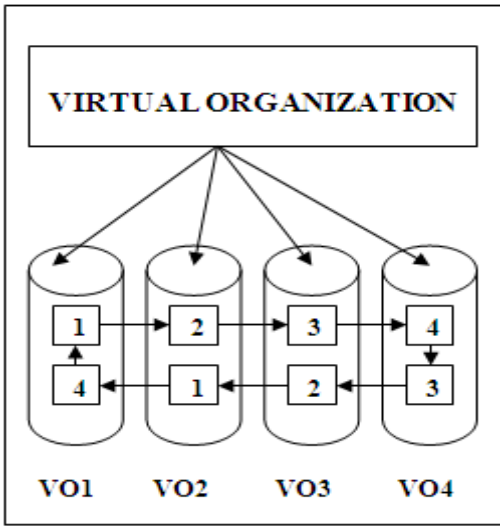


Fig 5: Vo Architecture

FLOW DESIGN:

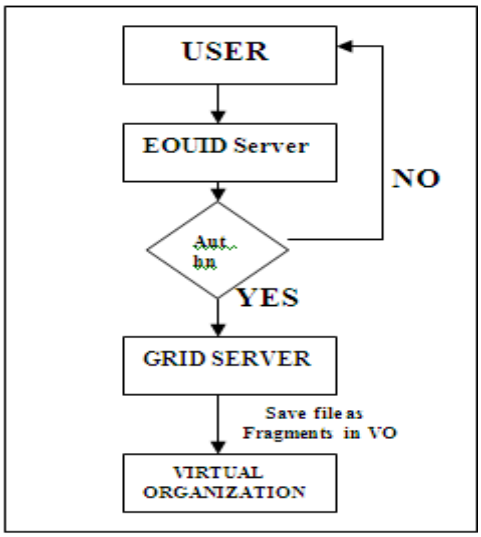
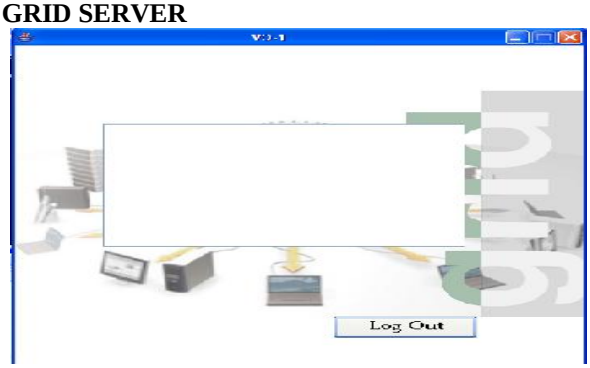


Fig 6: Flow Design

RESULTS:

USER LOGIN & AUTHENTICATION PROCESS

ONTOLOGY / GRID SERVER



VO GROUPS

X. CONCLUSION

This paper provides an approach of securing the data with protecting and controlling. The access to the decryption keys. It restricts the unauthorized users to access the data in a EOUID server. In addition this paper contributes to increasing the clarity of responsibilities and also to the creation of encryption and key management policies and practices.

REFERENCES

[1] L. Skitał, R. Słota, D. Nikolow, and J. Kitowski, "Methodology for virtual organisation design and management," presented at the EGEEUser Forum,CERN, Geneva, Switzerland, Mar. 1–3, 2006.
[2] Semantic Grid Platform in Support of Engineering Virtual Organisations. Matevž Dolenc, Robert Klinc and Žiga Turk.University of Ljubljana, Faculty of Civil and Geodetic Engineering,Jamova 2, SI-1000 Ljubljana, Slovenia Jan 2008
[3] Semantic Web-based Open engineering Platform (SWOP), http://www.swop-project.eu
[4] M. Hannus, *"Guidelines for Virtual Organisations"*, VOSTER Project Consortium, http://cic.vtt.fi/projects/voster
[5] Open Grid Services Architecture (OGSA),http://www.globus.org/ogsa
[6] I. Blanquer, V. Hernández, D. Segrelles, E. Torres.Long-term storage and management of encrypted biomedical data for real users in real organizations.
[7] William Stallings Cryptography and network security Third Edition.
[8] Towards Open Grid services Architecture. (2008). [Online]. Available:http:// www.globus.org/ogsa.
[9] The Web Services Resource Framework. (2008). [Online]. Available:http://www. globus.org/wsrf.
[10] Grid Security Infrastructure. (2008). [Online]. Available: http://www.globus. org/security/overview.html.