Enhanced way for Securing Data's Through Ontologies and Grids"

Kiran G M*,
Assistant Professor,
Department of CSE,
SIET, Tumakuru, Karnataka

Dr. Nalini N**,
Professor,
Department of CSE
NMIT,Bengaluru, Karnataka

ABSTRACT: Most of the existing servers like File servers, Network attached storage systems and etc are Used for storing and accessing data in the networks. These servers are building over single server architecture that is centralized manner. "Data Security" is a key requirement for these servers. But these file servers are becoming a major threat as it is subjecting to hacking. This paper presents a technique where data can be secured in an efficient manner and can be used in many applications, in existing system there was no security for stored data in the server side, so there were chances that third party can easily identify the data and chance of modifying the data was more, This paper present a model for storing the data for longer duration and managing the data in distributed environments.

Keywords: Grids, Ontology, Blow Fish, Information Object Storage, Cryptography.

I. INTRODUCTION

Ontology now a days has been brought in to the action by various agencies and medias in recent times following various attacks all round the world. It has been came to know that these hackers, apart from using state of art communication advancements and media, are utilizing cryptography and in addition Ontology to aid themselves with their objectives.

We all need privacy for the data stored in our system but since all our transactions takes place through a single server there were possibility of many attacks taking place across the world. So, there was no absolute protection guaranteed for stored data. So that hacker can easily identify the data and he can modify it, so we need to protect data from unauthorized access. This is achieved by using Ontology concept. In the Ontology concept, the data file is divided

into number of parts and each data part is stored into several different sub-systems. So

that hacker could not identify the data from different sub-systems, so we can avoid the modification or loss of data.

The main objective of file servers is to store data files. File server is nothing but a computer which is connected to a network that are having a purpose of providing possible locations for different shared disk access i.e., document files, text files, image documents, films, information constructs thus with respect to, that can be associated to a computer network. A file server basically does not perform any calculations or it does not run any program on behalf of their clients. It is primarily designed for retrieving data where computations are heavier in particular workstations.

File servers are generally used for offering some kind of securities to the system for accessing limits to the records to determined clients or particular gatherings. Document servers has basically got different security risks, since it is supporting the various transformation of unencrypted, text files which are clear or not modified over a network. These file servers are subjecting to the point of hacking. But Present security infrastructure in this type of servers is complex.

So this paper presents a security enhancing technique that can be used for storing and retrieving the data efficiently in a distributed environment in a server side, it provides an architecture that has four sub servers that stays behind the scene stores the equally fragmented and encrypted part of data each. Here the main server which is visible to the users presents only the view and does not store data.

This paper presents a technique for storing the data efficiently in a distributed environment. So our objective is to propose a cryptographic infrastructure to protect server data, to provide a flexible architecture, to propose a technique that can be adopted in different distributed environments.

II. RELATED WORKS

Kelvin Curran of the school of figuring and wise frameworks at university of Ulster analyzes how matrix registering is enhancing endeavor operations. Many large corporations such as Boeing and Pratt & amp, Whitney are currently using computational grids to enhance their operations. However future matrices will permit an association to exploit computational frameworks without having to develop a custom in-house solution. One case of an organization using the network is a centuries old financial publishing firm, Bowne & amp; co. Bowne launched a a humble generation lattice and therefore, the organization has cut in half processing time for key application that helps shared store clients meet monetary reporting controls. Boeing has utilized lattice grouping innovation to help in the aerodynamics analysis of their new set of rockets.

In both the above mentioned scenario data sharing were always deployed in an antagonistic situation and defenseless against various security threats. Authentication, Security, reliability, privacy was a major concern in various fields.

It is very difficult in an antagonistic situation and defenseless against various security multiple servers securely. Therefore we will try to overcome the above mentioned problems by using a combination of grid and ontological infrastructure in our proposed projects.

III. PROBLEM STATEMENT

The present security infrastructure in file servers is complex. Thus, there is a requirement of an efficient, simple mechanism of security infrastructure for file server data.

In present systems the data in file server are stored using the concept of single server which are subjecting to hacking in many environments. So "the main problem statement focus of the project work is to encrypt the file server data files, divide the data file into four equal fragments and store the each fragment in four sub servers instead of storing it in single server. In proposed system, only the server with the front-end services is directly engaged with the users while sub servers are stayed behind the scene. Hence it is possible to directly strengthen the existing server architectures.

IV. SOLUTION TO THE PROBLEM

In existing system, there was no security for the data that are stored in the servers. So that the hacker can easily identify the data and he can modify it. So we need to protect data from unauthorized access. This is achieved by using Ontology concept. The security system mainly deals with securing file server data using cryptographic infrastructure and storing data in the four sub servers which runs behind the scene. The security system work should be compatible with the windows operating systems.

The main objective of this paper is,

- To design an efficient model for storing and managing the encryption of data in different distributed environments.
- To propose a model that is applicable with current grid middleware's.
- Contributing to the society in proposing a practically implementable solution to overcome the problem of existing system by using grids and ontology.
- Establish, at institute or university level, leading to one of the best projects at the institute/university level.

V. SYSTEM ARCHITECTURE

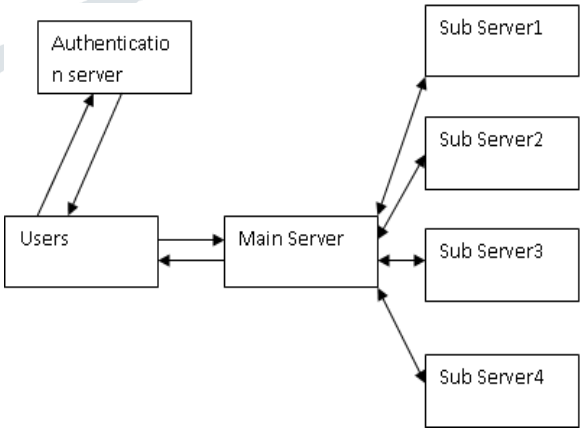

Figure 1: Client- Server Ontology based system Architecture

The Architectural diagram as shown in the figure above consists of seven components such as User login Interface, Authentication server, main server, Sub server1,Sub server2, Sub server3,Sub server4. UI segment comprises of a login form that inputs username and password. Authentication server component authenticates the user. Main server component accepts the data file from the user, encrypts the data file, divides it into four equal parts and stores each part into sub servers. Sub server components stores each fragments.

The repository services are provided by the model by using an IOS. The encrypted information objects required by various groups of the virtual organization are stored in the repository. IOS also helps in maintaining the relationships between the objects and the ontologies by using an encrypted object unique identifier (EOUID).

In addition ontologies are used for searching, filtering and indexing encrypted objects in an environment of virtual collections.

Some of the firms who are in active in use of grids and ontologies are:

Butterfly.net and IBM want to utilize the benefits of framework figuring consolidated with Blade Centers to enhance the path in which clients play arrange construct PC amusements with respect to play station 2 consoles.

IIT Kanpur is conveying network processing equipment and programming from SUN India, for its PC focus. The establishment will make it the largest AMD opteron HPTC education segment in India. These organizations utilized lattice registering adequately to accomplish extensive cost and efficiency points of interest.

The efforts of Anna University, Madras Institute of Technologies (MIT), who joined forces with C-DAC in creating grid technologies furthermore, applications, merit saying as they are moreover making grids interfaces available in Indian languages. **Garuda India: The National Grid Computing Initiative** – C-DAC has been supported by the information technology department (DIT), India to deploy the nationwide computational grid GARUDA.

Apollo hospitals are using the concept of ontologies for storing the patient information.

SBI, Axis, Hdfc and so on banks are using ontological infrastructure using IOS for storing details related to their banks.

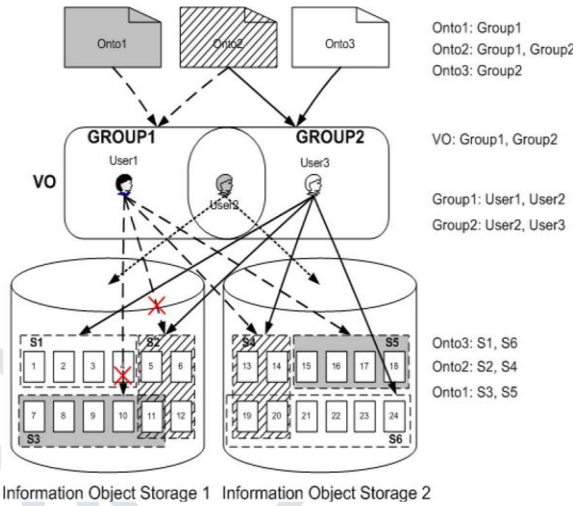

Figure 2: Access control relation among various ontologies

VI. SYSTEM IMPLEMENTATION

1. Establishing communication session between clients with a main server by socket programming.
2. Creating an efficient GUI for client.
3. Encrypting the data file.
4. Dividing the data file into four equal fragments.
5. Having control of enability/ disability of server software functionalities.
6. Sending each fragment to each sub server.
7. Retrieving each fragment from the sub servers.
8. Decrypt the data file and display to user.

VII. RESULTS

Data's are initially encrypted and were stored in IOS. Data's that were not unencrypted were also stored in an IOS to indicate the differences between encrypted and unencrypted data's in an object. The possibility of retrieving the data efficiently in the client and server sides is efficiently measured.

VIII. CONCLUSION

One of the main security threats is the ability of malicious software or attackers to steal important or confidential information from the servers. The security system work highlights about the noble intentions of the security manager of any

organization to implement an efficient and secured data storage architecture that includes cryptographic infrastructure. As seen in our paper, the Single Server architecture are the one who are creating these security provisos in the corporate network, in this way posturing peril to the entire server data.

This paper results for an application which can to be installed in single server architecture system. The system is designed in such a way that the server data is divided in to four fragments and each fragments are stored in sub servers which runs behind the scene. This paper is entirely designed with the help of Java. This paper has got the potential to secure server data by storing the server data in sub servers which runs in back end. Not only this, the security system work also aims to divide the server data into four fragments and encrypt. The encrypted data is stored in sub servers. In our system only the servers with the front-end services are directly engaged with the users while sub servers are stayed behind the scene. Hence it is possible to directly strengthen the existing server architectures.

REFERENCES

[1] I. E.Magnin and J. Montagnat, "The grid and the biomedical community: Achievements and open issues," presented at the EGEE User Forum,CERN, Geneva, Switzerland, Mar. 1–3, 2006.

[2] J.M. Schopf, "Grids: The top ten questions," *Sci. Program.*, vol. 10, no. 2, pp. 103–111, 2002.

[3] Ł. 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.

[4] I. Blanquer, V. Hernandez, and J. D. Segrelles, "An OGSA middleware for managing medical images using ontologies," *J. Clin. Monit. Comput.*, vol. 19, pp. 295–305, Oct. 2005.

[5] *Digital Imaging and Communications in Medicine (DICOM)—Part 10: Media Storage and File Format forMedia Interchange*,National Electrical Manufacturers Association, Rosslyn, VA, 2008.

[6] I. Blanquer, V. Hernandez, and D. Segrelles, "TRENCADIS—A WSRF grid middle ware for managing DICOM structured reporting objects," *Stud. Health Technol. Inf.*, vol. 120, pp. 381–391, 2006.

[7] Ciberinfraestructura Valenciana deImagenM´edica Oncol´ogica (CVIMO). (2008). [Online]. Available: http://www.grycap.upv.es/cvimo

[8] V. Breton, K. Dean, and T. Solomonides, Eds., "The Healthgrid white paper," in *From Grid Healthgrid—Proc. Healthgrid 2005, Stud. Health Technol. Inf.* vol. 112. Amsterdam, The Netherlands: IOS Press, pp. 249–321.

[9] J. Montagnat, A´ . Frohner, D. Jouvenot, C. Pera, P. Kunszt, B. Koblitz, N. Santos, C. Loomis, R. Texier, D. Lingrand, P. Guio, R. Brito Da Rocha, A. Sobreira de Almeida, and Z. Farkas, "A secure grid medical data manager interfaced to the gLite middleware," *J. Grid Comput. (JGC)*, vol. 6, no. 1, pp. 45–59, Mar. 2008.

[10] C. Blanchet, R. Mollon, and G. Del´eage, "Building an encrypted file system on the EGEE grid: Application to protein sequence analysis," in *Proc. 1st IEEE Int. Conf. Availability, Rel. Security (ARES 2006)*, pp. 965–973.

[11] EGEE: Enabling Grids for E-sciencE (Phase I and II). FP6 European IST Project, Contract Number INFSO-RI-508833. (2008). [Online].Available: http://www.eu-egee.org

[12] World Wide Web Computing Grid. Distributed Production Environment of Physics Data Processing. (2008). [Online]. Available: http://lcg.web.cern.ch/LCG

[13] S. Varrette, J. L. Roch, J. Montagnat, J. M. Pierson, L. Seitz, and F. Leprevost, "Safe distributed architecture for image-based computer assisted diagnosis," presented at the IEEE Int. Conf. Pervasive Serv. (ICPS 2006), Workshop Health Pervasive Syst., Lyon, France, Jun. 2006.