



Accessing the Data Security Model in Distributed System

Manu Agarwal
Deptt. Of Computer Science
Govt.Girls Polytechnic, Bareilly, India

Gaurav Agarwal
Deptt. Of Computer Science
Invertis University, Bareilly, India

ABSTRACT

This research deals with the comparative study of distributed system and client/server computer system, placing a special emphasis is on security system. The researches describe the data security in these systems by describing them; examine their issues, challenges and presenting the adequate solutions. We have selected four type of distributed system and included a report on the basis of authorization, authentication, encryption, access control.

Keywords

Distributed System, Data Security, Authentication, Authorization

1. INTRODUCTION

When there are some systems works in the collaborative manner with other system for the purpose of communicating each other for, processing data transfer, data storage etc. these systems may be scattered by distance it is commonly known as a distributed system. Researchers defined different definitions for the distributed system Colourise et al., have defined a distributed system as “a system where the hardware and software components have been installed in geographically dispersed computers that coordinate and collaborate their actions by passing messages between them [1] etc. According to these definitions given by researchers a distributed system have been built with the objective of attaining the following.

- Transparency
- Openness
- Reliability
- Performance
- Scalability

To achieve these main objectives of distributed system attention must be pay on a fundamental requirement of system i.e. security at every stage of designing, implementation, operation and management by the user [2].

As every organization is concerned about protecting their data against intruders so security has become more complicated for the organization. For protecting their data and information against intruders organizations set up a security system which involves the identification of risks, sufficient security for organization and security awareness. In this paper, we presented the implementation of security over different type of distributed systems.

1.1. Classification of Distributed System

For our research work we have taken the four types of distributed system as follows and present a security model of mentioned distributed system.

- Cluster Computing.
- Grid Computing.
- Distributed Storage Systems.
- Distributed databases.

1.1.1. Cluster Computing

A cluster is known as when different computers are grouped together to form a set in such a manner that they can form a pool of resources. When any task is assigned to the cluster it would be run on all the system in the set by parallel fashion. In the cluster computing the whole task is broke in smaller tasks. Then these outputs from different machines would be combined to form the final result [3]. It helps organization to increase the computing power by availing the best part of technology. These clusters are used to run engineering and industrial applications which requires high throughput processing [4]. The architecture of cluster computing is as shown below.

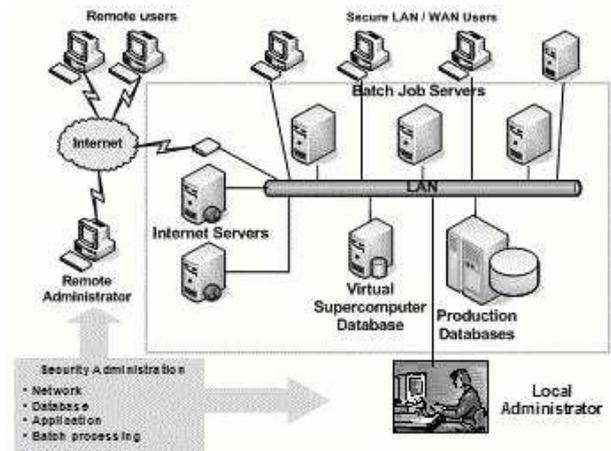


Fig.1 Cluster Computing Architecture

1.1.2 Grid Computing

When a large number of small computers are brought together to form a type of virtual supercomputer. This type of computing system is known as the grid computing system. The benefit for this virtual super is that it can perform the tasks which may be large for small computers. The virtual super computer can perform these tasks in a reasonable time. Grid is defined as a parallel and distributed system that is

capable of selecting, sharing, and aggregating geographically distributed resources dynamically at runtime based on their availability, capability, performance, and cost meeting the users' Quality of Service (QoS) requirements [5]. Figure 2 shows Grid System distributed across heterogeneous computing platforms which is used to perform some intensive scientific, mathematical and academic problems through the computing process.

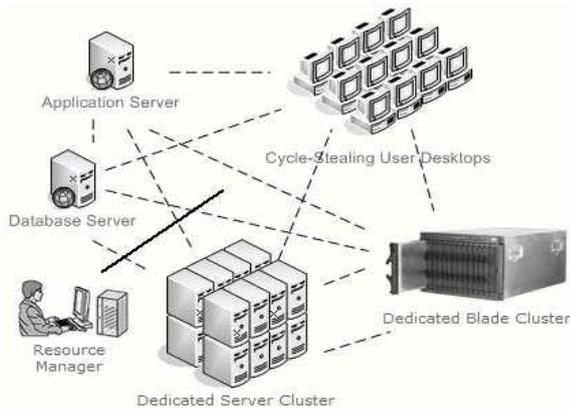


Fig. 2 Grid Computing System

1.1.3 Distributed Storage System

The distributed storage systems were designed to protect data across multiple devices in that case if disk failure through redundant storage. It makes data available closer to the user in distributed system [6]. The types of distributed storage system are Redundant Array of Independent Disks (RAID), Centralized RAID, Network Attached Storage (NAS) and Storage Area Network (SAN). In all above SAN and NAS are the popular distributed storage techniques. Fig 3 shows the typical arrangement of distributed storage system.

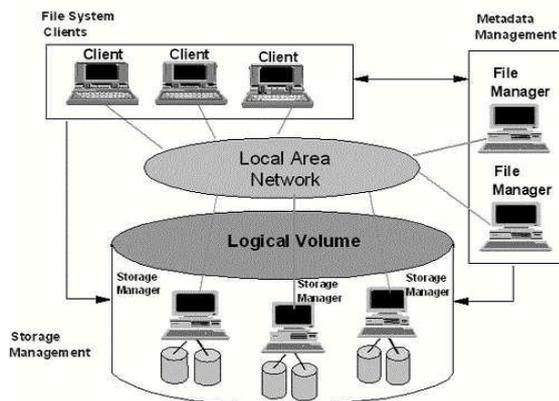


Fig 3 Architecture of Distributed Storage System

1.1.4 Distributed Database System

In the distributed database system user collect independent database systems across different computers and store this data collaboratively in a manner that user can access data from anywhere as it is stored locally [7]. Fig 4 shows the arrangement of distributed database system.

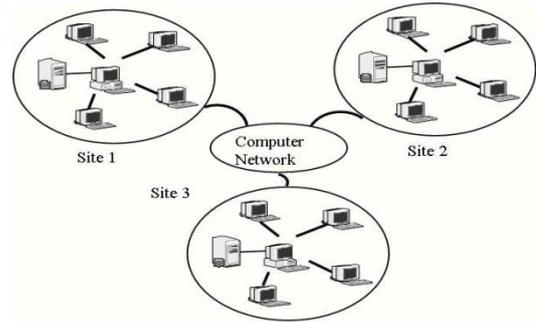


Fig 4 Arrangement of Distributed Database System

2. SECURITY IN DISTRIBUTED SYATEM

As data is distributed across different networks by the distributed systems so security becomes the most important issues in these systems. Data is distributed via public networks so the data and other resources like storage devices, processors etc can also be attacked by hackers. Researchers define different security aspects for these systems. As for the computing clusters Li and Vaughn proposed security vulnerabilities of computing clusters using exploitation graphs (e-graphs). They have modelled several attacks that can be carried on all three pillars of security namely, confidentiality, integrity and availability. They have shown that e-graphs can be simplified based on domain knowledge such as cluster configurations, detected vulnerabilities, etc. they further state that this technique could be used for certification of clusters with the help of a knowledge base of cluster vulnerabilities [8]. For grid computing the security is based on public key infrastructure (PKI). Kerberos password etc [9]. Hasan et al., introduced threat model named CIAA threat model. This model addresses all the security issues related to distributed storage system namely Confidentiality, Integrity, Availability and Authentication [10]. For the security purpose of distributed database systems Zubi designed a model which improved the scalability, accessibility and flexibility while accessing various types of data. He has worked with access control, confidentiality, reliability, integrity and recovery to manage the security of a distributed database system [11].

3. SECURITY COMPONENTS IN DISTRIBUTED SYSTEM

There are four main security components of distributed system: security authentication, authorization, access control and encryption. Basically authentication provides a service like password which works with the authentication server for linking with the network. Authorization examines the identity of client and server over the network by the software servers. In the distributed system the access control is done by the matrices, access lists, capabilities lists which define access authorization to the computer resources for the user. Also in distributed system the encryption is done by the algorithms like RSA, PGP, DES based on public and private key [12].

4. PROPOSED MODEL FOR DISTRIBUTED SYSTEM SECURITY

Based on these security components discussed above we have propose some security models for distributed system. In our work we have presented the security model based on access control which operates on local area network environment. Proposed model aims to the many work stations and the users at different locations it supplies passwords for authorization and authentication to users and station of different networks. Our model is basically suitable for the systems where a large number of transactions like updating and modification is done in a time. For an example a railway reservation systems in which there are many transactions and queries like reservation and cancellation, modification and updating of seats. The clerk using these data system may face such problems like the accounts with foreign currency, securities etc. when a clerk will deal with one transaction for example allocation of seats all other transaction will be blocked and the chances of attacks on system may arise. So the model that we are presenting here is the solution of all such type of problems. The model encompasses the users of work stations and the transactions they carry out. Figure 5 describe the software architecture of the model which is based on client/server architecture. The software server works on each workstation as an independent application. In the presented model various clients will get the security services via the interface based on security. The main requirement is that this security interface must be incorporated in each application (client)

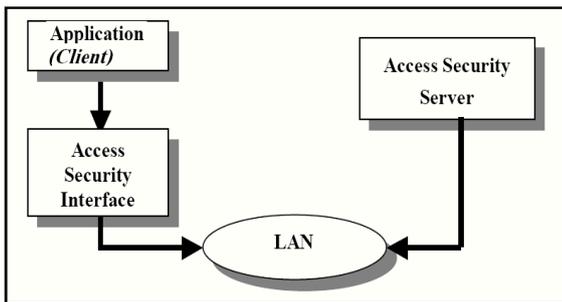


Fig 5 Distributed Software Security Model based Client/Server Technology.

There are some basic rules suggested for access the security in the system which is defines as below [13].

- Users may operate from all stations, it is not necessary that their maximum authority exceed from the maximum authority granted by the station.
- For caring any transaction the station must have proper authorization. The rules define for accessing the security can be learned as the fig.6

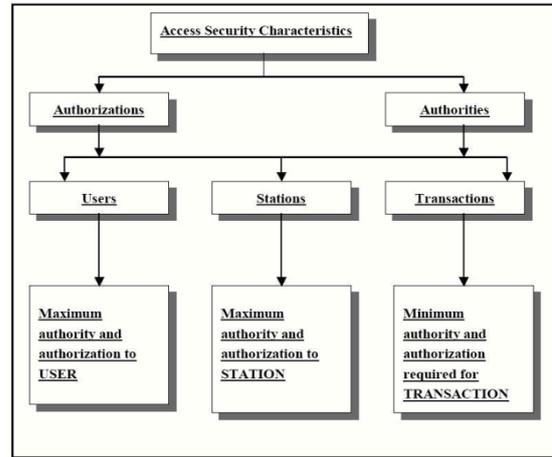


Fig.6. Basic characteristics for accessing security in distributed systems

The proposed model for implementing the security in the distributed system work on the three layers of communication. First one is the communication layer which deals with the communication between client to client, responsible for the sending and receiving the data and information over the distributed system.

Second layer is the talk layer which is responsible for identification and analysis of the message received and sent by all the clients in system. This layer also deals with the reply and release message for completion of transaction. Third and last layer known as the application layer which handles requests service regarding the user and handles requests for transaction services. Fig.6 describes the software architecture for access security in distributed system.

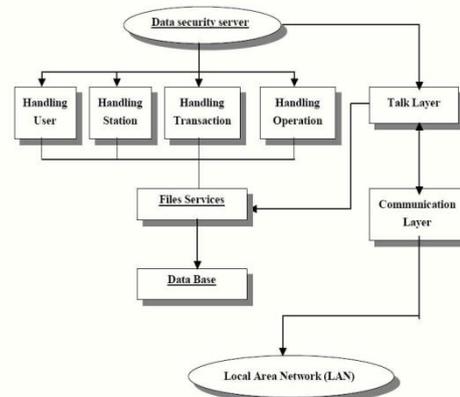


Fig 6 Software architecture for accessing security in distributed system

5. CONCLUSION

In the work presented here different type of distributed systems has been discussed in terms of security. We have taken four type of distributed systems and the security issue faced by them also been discussed. We have proposed a model for accessing the security in the distributed systems based on client/server approach. The software architecture of model is based on the different layers and it gives the solution for all security components for distributed system like authentication, access control, encryption etc.



6. REFERENCES:

- [1] George Coulouris, Jean Dollimore and Tim Kindberg, Distributed System- Concepts and design, 4th ed. London England: Addison- Wesley 2005.
- [2] Andrew S Tnaenbaum and Maarten van Steen, Distributed system: Principal and Paradigms, 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007
- [3] Mark Baker and Rajkumar Buyya, “Cluster Computing: Architecture and System- Volume 1 Prentice Hall, 1999, ch.1 pp-3-47
- [4] Chee Shin Yeo, “Utility-based Resource management for Clusters Computing,” the university of Melbourne, Australia, PhD Thesis 2008.
- [5] Rajkumar Buyya and Srikumar Venugopal, “Market Oriented Computing and Global Grids: An Introduction,” in Market Oriented Grid and Utility Computing, Rajkumar Buyya and Kris Bubendorfer, Eds Hoboken, NJ, USA: John Wiley & Sons, Inc, 2010, ch 1, pp.3-27
- [6] Yuchong Hu, Yimlong Xu, Xiaozhao Wang, Cheng Zhan, and Pei Li, “ Cooperative Recovery of Distributed Storage Systems from Multiple Losses with Network Coding,” *IEEE journal on Selected Areas in Communication*, vol. 28, no. 2, pp. 268-276, February 2010
- [7] Ali Safari Mamaghani, Mostafa Mahi, Mohammad Reza Meybodi, and Mohammad Hosseinzadeh Moghaddam, “ A Novel Evolutionary Algorithm for Solving Static Data Allocation Problem in Distributed Database System,” in *Second International Conference on Network Application, Protocols and Services (NETAPPS)*, Alor Setar, Kedah, 2010, pp. 14-19
- [8] Wei Li and Rayford B Vaughn, “ Cluster Security Reaserch Involving the Modeling of Network Exploitations Using Exploitation Graphs,” in *Sixth IEEE International Symposium on Cluster Computing and the Grid Workshop (CCGRIDW’06)*, Singapore, 2006, pp. 26-36.
- [9] Yuri Demchenko, Cees De Laat, Oscar Koeroo, and David Groep, “ Re-thinking Grid Security Architecture,” in *IEEE fourth International Conference on eScience, 2008 (eScience ’08)*, Indianapolis, IN, USA, 2008, pp. 79-86
- [10] Ragib Hasan, Suvda Myagmar Adam J Lee, and William Yurcik, “Toward a threat model for storage system,” in *Proceedings of 2005 ACM Workshop on Storage Security and Survivalist (StorageSS’05)*, Fairfax, VA, USA, 2005, pp. 94-102
- [11] Zakaria Suliman ZUBi, “ On Distributed Database Security Aspects,” In *International Conference on Multimedia Computing and System*, Ouarzazate, Morocco, 2009, pp. 231-235
- [12] White, D (1999), Distributed system security, *DBMS*, 10, pp. 44-48.
- [13] Amoroso, E. (1994), *Fundamentals of Computer Security Technology*, ch. 7, Prentice-Hall, Englewood Cliffs, NJ.