A Survey on Distributed System Security, Implementation Issues and Challenges

M. Janardhan[1], M. Fasiha Anjum[2], J. Manasa Lakshmi[3]
[1, 2, 3]Department Of Computer Science And Engneering
[1, 2, 3]G. Pullaiah College of Engineering and Technology

Abstract*-This paper represents evolution of security y in distributed system and challenges related to security in those systems. Nearly new distributed system is deemed of four types. Different techniques in security as explained as secure channel, cryptographic encryption and decryption etc. Implementation of security has been as judgmental point.*

I. INTRODUCTION

The security in our data will get from providing authentication, confidentiality, authorization and also done by provide cryptographic-based technique of the data recent trends focused on the [1]. Some attackers attempt to modify or misuse the information depending on the actions performed by them. Active attack such as message tempering (changing the content in message), eavesdropping (someone trying to steal unauthorized information), masquerading (making assumptions on the identity of users), replaying message and Daniel of service.

The reliability in the system depends on the confidently and authentication. However, this paper say about the system is safe or not. Next security system models are explained in distributed system [2]. The Principal goals in distributed system include transparency, failure, and relocation [11], quality of service to the users.

A. DISTRIBUTED SYSTEMS:

Till date we find different methods of distributed systems based on their operations [2].

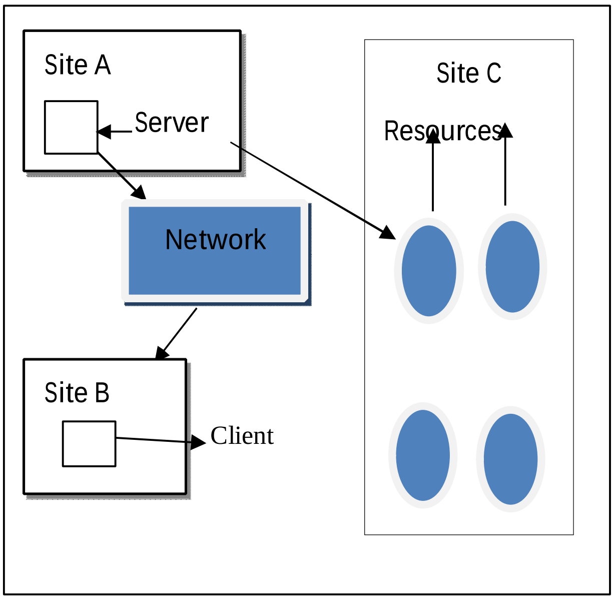


Figure 1. Distributed System

The following are some of the most popular distributed systems in use today.

1. Cluster computing

A cluster is connected with a set of computers that perform communicating over a high-speed network that can work and present itself as a single computer to the users. A cluster is commonly connected to a centralized area network. It helps organizations to increase their computing power using the standard and commonly available technology [2]. The commodity items are easily available at low cost like hardware and software.

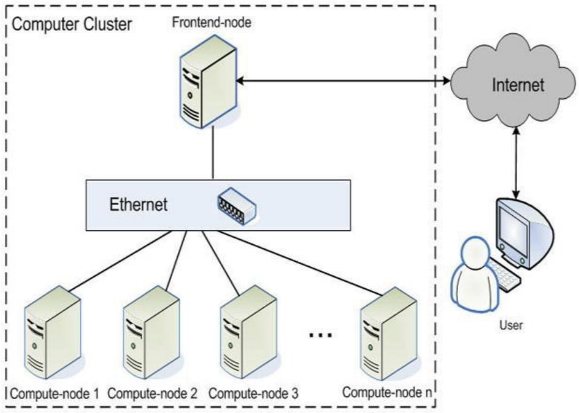
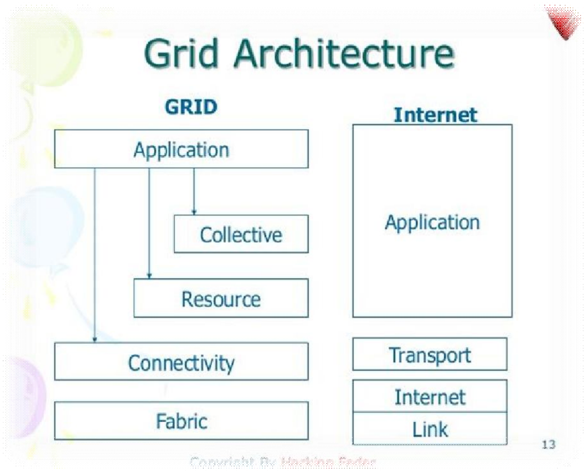


Figure 2. Cluster Computing

2. Grid computing

Grid computing is similar to cluster computing nut in grid large number of computers are connected as virtual supercomputers. Virtual supercomputer can perform the task of large computer with greater efficiency that single system.



Grid Architecture

GRID

Application

Collective

Resource

Connectivity

Fabric

Internet

Application

Transport

Internet

Link

13

Copyright By Hacking Feder

Figure 3. Grid computing

3. Distributed storage systems

The successive increase in storage, bandwidth and computation resources like speed, availability, consistency along with number of peer network nodes. The issue in distributed storage system is fault tolerance and security in the user's information. Fault tolerance can make server "stateless" and logging or transactions easy. There are mainly four types of distributed storage systems as proposed in[2]. There are many distributed storage networks like, RAID, SAN, NAS, where NAS and SAN are commonly used and popular among four.

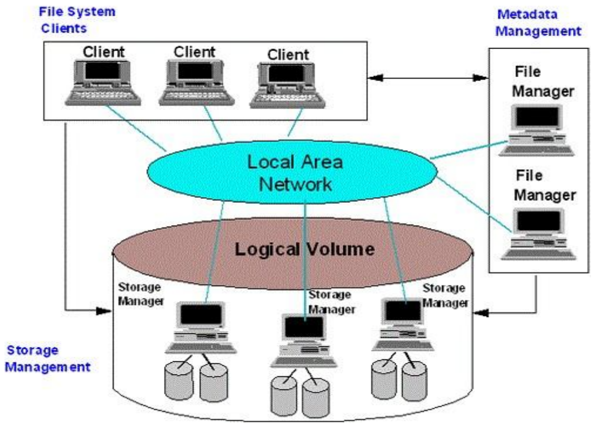


Figure 4. Distributed Storage System

4. Distributed Database System

It is a collection of several computers networks in collection with stored data in such that users can access the data from anywhere at any time. The distributed management system acts like software that provide access for transferring the information to the users [10].

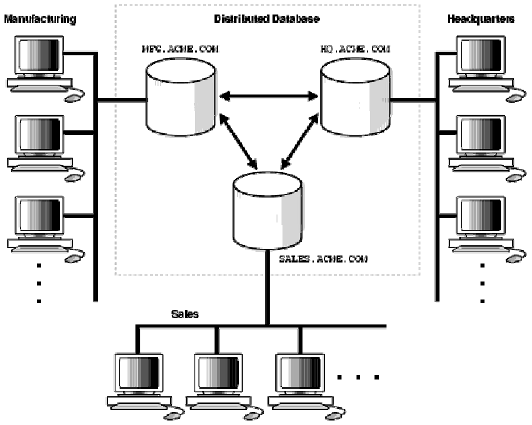


Figure 5. Distributed database system

II. SECURITY APPROACHES IN DISTRIBUTEDSYSTEMS

Many papers have stated distributed system but none of them have got the common meaning. The Common goal in distributed system, is solving by a large computational problem. Distributed system structure includes individual computer with network topology, network latency, number of computer. Every individual computer has limited and incomplete system and also has only one input component.

There are different strategies and approaches order to protect the communication between client and server we use some security techniques like secure channel, access control through authentication, confidentiality and many other, the security and privacy in user’s data the information stores in different system over different site in contact through computer networks.

A. Authentication Based Security

The path authentication has been proposed in, M.Shehab,et [3]. Path Discovery algorithm has been proposed to securely discover the paths in collaboration environment. This technique Directed acyclic graph (DAG) which is a systematic security driven scheduling architecture. Authentication Serves is provided by new password based authentication approach. This Approach is to validate the user’s data from the third party.

Three-factor authentication is a simple technique to smart-card-based, password authentication. This approach has a security factor which require biometric characteristics, [1,3,4].

B. Trust based security approaches

Ensuring and enhancing the system security plays a important role in distributed system. This Is achieved by computing trust like peer to peer systems. trusted environment principal is to identify the user in the system at each level.[5] has proposed password based methods to identify the users of the system for authentication and authorization.

Rapid growth in the trust models has increased the security in distributed system. An extended d-s theory-based trust model (exdstm) is developed. Other ds theory models are proposed.

C. Access Control-Based Security

Access control have been emerged since the distributed systems have started accessing and sharing the multiple resources. Access Control maintains the relationship between permissions, subject, object and operations.

The main objective of the access control is whether the source1 (human, process, computer etc.) can perform operation on source2 (read, write, execute etc.) determining their policies. The main aim of access control the proper writing and to provide only useful permissions. There Are three widely spread access control models, they are[3].

1. Lampson's matrix and discretionary
2. Bell-lapadula, lattice-based and mandatory access control
3. Role-based access control

1. Lampson's matrix and discretionary

This model was established in 1960's by lampson, after introducing notions such as subject, object and matrix. A matrix is represented by [i,j], i denotes the rows capability list and j denotes columns access control list which define permissions.

2. Bell-lapadula, lattice-based and Mandatory access control

The basic principal in mandatory access control is to deal with classification of the computer system[1], according to the clearness and object classification of the user's.

3. Role-based access control

In role-based access control the permissions are associated with role but the permissions are not directly assigned to the user’s. Its Main aspect is to reduce the complexity and one important feature in role base access control is that here roles are hierarchical. The Definition of role-based access control is quoted from [6] in 1996:” role is a job title or function within an organisation with some associated semantics”.

D. Cryptography based approaches:

This approach is used to develop the secure distributed systems which use the various applications like public key infrastructure and role-based access control. This Approach uses the public key cryptography, software agents and xml binding technologies for security. The main encryption in symmetric algorithm known as Data Encryption Standard (DES), and also Advance Encryption Standard (AES).

The security in distributed system is mainly device level control that has been proposed in [7].

E. Policy based approaches

The policy-based approach uses the domain specific language for implementation of security policies in distributed system. policy is to provide the security to the data and also its main object is to provide authorization to the data.

F. Pattern based security

This approach contains the different types of security approaches that is based on security methodologies. Different Types of security approaches are reported by[9].

G. Quorum based security systems

As discussed by [9], this approach is used to solve the problems of data inconsistency in distributed fault-tolerance. In this the role ordering schedule also introduced for transactions.

H. Other security-based approaches

A mobile agent-based security model has been proposed. This Model explains and analyse the strength of security and various threats. Self-protection is used to detect the illegal behaviour in intrusion is explained in[9]. The Efficient collaboration in between security and privacy for distributed system security has been discussed [1].

Genetic algorithm has been applied in order to optimize the distributed security system. A heterogeneity approach and novel heuristic algorithm, which helps to optimize the execution of task without risk attacker rate.

I. Secure channel

The other commonly now word for a secure channel is Schannel, which contain set of security protocols to protect the communication between server and client that is provided through authentication and secure, private communication through encryption. 1. Authentication Through Secure Channel

Authentication for the user is done through secure channel by secret key applying encryption for user's message integrity and confidentiality. Authentication based methods on session key by authentication based on shared keys authorship, authentication using a key distribution centre, authentication using public key encryption.

III. ISSUES AND CHALLENGES INDISTRIBUTED SYSTEMS

Different papers have discussed about different issues and problems faces in [1,11]. This paper simplifies all the basic challenges and problems in distributed systems. In order to maintain security and trust in distributed system we must solve many critical issues [10] like:

1. Developing security metrics.
2. Cryptographic techniques like single key or public key, in user information.
3. Determining the system security.
4. Identification of topology in the system.

Design Issues related distributed system

1. Openness: The checks if the system can Be rebuilt and extended without disturbing other components.
2. Security and privacy: The major components of security in user's information are: confidentiality, integrity and availability. How to apply security policies to independent system is a greater issue as proposed in[10].
3. Transparency: It is used to hide the information from the users. Several aspects of distributed system location transparency, migration transparency, replication transparency, parallelism transparency etc.
4. Failure handling: When faults occur in hardware or software[11], program may start giving incorrect results or may stop the execution of program. Handling the control if one component fails while others continue to function.
5. Quality of Service: How to determine nonfunctional properties of system that affect the quality of the service experienced by clients and users are reliability, security and its performance.

IV. CONCLUSION

This paper describes what a distributed system is and the basic purpose of different kinds of distribution. Their implementations and security approaches like authentication confidentiality secure channel through authentication, cryptographic approaches. Security issues and challenges in distributed system is explained in this paper.

REFERENCES

[1] Vijay Prakash, Manuj Darbari" A Review on Security Issues in Distributed Systems" International Journal of Scientific & Engineering Research Volume 3, Issue 9, September-2012.

[2] Mohamed Firdhous Faculty of Information Technology, University of Moratuwa, Moratuwa, Sri Lanka, International Journal of Computer Information Systems, Vol. 2, No. 2, 2011.

[3] M. Shehab, A. Ghafoor, E. Bertino, Secure collaboration in a mediator free distributed environment, IEEE Transactions on Parallel and Distributed Systems, vol. 19, no.10, pp.1338-1351, 2010.

[4] X. Huang, Y. Xiang, A. Chonka, J. Zhou, R.H Deng, A generic framework for three factor authentication: Preserving security and Privacy in Distributed Systems.

[5] Romuald Thion University of Lyon, France" Access Control Models".

[6] Ravi S. Sandhu, Edward J. Coyne, Hall.Feinstein," Role-Based Access Control Models", Volume 29 Issue , Feb-1996.

[7] Y. Xu, L. Korba, L. Wang, Q. Hao, W. Shen, S. Lang, A security framework for collaborative distributed system control at the device level, IEEE International Conference on Industrial Informatics, 2003, pp.192-198.

[8] A. V. Uzunov, E. B. Fernandez, K. Falkner, Securing Distributed systems using patterns: a survey, Computers and Security,in press

[9] Prof. Steve Wilbur Room G03," Distributed Systems Security ", Ext. 1397, 19 November, 2000.

[10] Kamal Sheel Mishra, Anil Kumar Tripathi "Some Issues, Challenges and Problems of Distributed Software System". , Vol. 5 (4) , 2014.

[11] Reza NayebiShahabi,"Security Techniques in Distributed Systems",volume 3(2), 2015.