© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 01 | January - March 2016

IMPLEMENTATION OF ADHOC NETWORK TO ENABLE CENTRALIZED AND DISTRIBUTED COMPUTING

[1]Savita Sheoran, [2]Mr. Gagandeep, Dept. of CSE , PPIMT Hissar

Abstract: This Research presents a comparative study of distributed and centralized systems and the security issues associated with those systems. Four commonly used distributed systems were considered for detailed analysis in terms of technologies involved, security issues faced by them and solution proposed to circumvent those issues. Finally the security issues and the solutions were summarized and compared with each other. When systems work in this collaborative fashion with other systems that are geographically scattered over wide distance it is commonly known as a distributed system. In literature, researchers have used diverse definitions to outline what a distributed system is.

Keywords *– Centralized System*, Distributed systems, security, Cryptography, Encryption, Decryption

[I] INTRODUCTION

Ad hoc is a word that originally comes from Latin and means “for this” or "for this situation."

It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station.

For example, if you need to transfer a file to your friend's laptop, you might create an ad hoc network between your computer and his laptop to transfer the file. This may be done using an Ethernet crossover cable, or the computers' wireless cards to communicate with each other. If you need to share files with more than one computer, you could set up a mutli-hop ad hoc network, which can transfer data over multiple nodes.

Basically, an ad hoc network is a temporary network connection created for a specific purpose (such as transferring data from one computer to another). If the network is set up for a longer period of time, it is just a plain old local area network (LAN).

Centralized computing is computing done at a central location, using terminals that are attached to a central computer. The computer itself may control all the peripherals directly (if they are physically connected to the central computer), or they may be attached via a terminal server. Alternatively, if the terminals have the capability, they may be able to connect to the central computer over the network. The terminals may be text terminals or thin clients, for example. It offers greater security over decentralized systems because all of the processing is controlled in a central location. In addition, if one terminal breaks down, the user can simply go to another terminal and log in again, and all of their files will still be accessible. Depending on the system, they may even be able to resume their session from the point they were at before, as if nothing had happened.

This type of arrangement does have some disadvantages. The central computer performs the computing functions and controls the remote terminals. This type of system relies totally on the central computer. Should the central computer crash, the entire system will "go down" (i.e. will be unavailable).

Another disadvantage is that central computing relies heavily on the quality of administration and resources provided to its users. Should the central computer be inadequately supported by any means (e.g. size of home directories, problems regarding administration), then your usage will suffer greatly. The reverse situation, however, (i.e., a system supported better than your needs) is one of the key advantages to centralized computing.

[2] LITERATURE REVIEW

In December 2012 Network Security Using Cryptographic Techniques by Sumedha Kaushik, Ankur Singhal :

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions,

characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use:

Cryptographic techniques; hence our focus is on this area Cryptography. Cryptography is an emerging technology, which is important for network security. Research on cryptography is still in its developing stages and a considerable research effort is still required for secured communication.

C. Sanchez-Avila et.al analyzed the structure and design of Rijndael cipher (new AES), remarking its main advantages and limitations, as well as its similarities and dissimilarities with DES and T-DES. Finally, a performance comparison among new AES, DES and T-DES for different microcontrollers has been carried out, showing that new AES have a computer cost of the same order than the one needed by T-DES [4]. A. Murat Fiskiran et.al showed some cryptographic algorithms that have properties that make them suitable for use in constrained environments like mobile information appliances, where computing resources and power availability are limited characterization of the instructions executed by these algorithms, and demonstration that a simple processor is sufficient.

Susan et.al concluded that the Security field is a new, fast moving career. A focus on security stabilizes course material, reduces worry about student hacking, and helps to provide students the skills necessary to become security analysts. It also defines the set of skills required by Network Security analysts as network Security skills emphasize business practices, legal foundations, attack recognition, network optimization and describes active learning exercises that assist the students in learning these important skills. This actually summarized all the skills relating to network security, and discussed active learning exercises that assist students in learning these important skills. Main focus was on security information skills that are to be used in securing the network

Neetu Settia et. al discussed the security and attack aspects of cryptographic techniques and also discussed the dominant issues of security and various attacks. Finally, bench marked some well-known modern cryptographic algorithms in search for the best compromise in security. In this paper,CrypTool was used as a simulator to conduct the experiments and to get the result.

Punita Meelu et.al presented the fundamental mathematics behind the AES algorithm along with a brief description of some cryptographic primitives that are commonly used in the field of communication security since AES provides better security and has less implementation complexity and has emerged as one of the strongest and most efficient algorithms in existence today.

Zhang et.al focused on application level attacks and explores how the packet payload can be used for identifying application level attacks. It also discusses the current status of network anomaly detection, and emphasized the importance of payload based detection research using existing problems, and proposed an efficient method to detect payload related attacks. The method is divided into a training phase and a detection phase

Yudhvir Singh et.al considered various attacks such as simulation based attacks on cipher text only, known plain text and manual analysis in the network. The simulation based information theory tests such as Entropy,Floating Frequency, Histogram, N-Gram, Autocorrelation and Periodicity on cipher text were done. The simulation based randomness tests such as Frequency Test, Poker Test, Runs Test and Serial Test on cipher text were done.

Sumedha Kaushik, Ankur Singhal wrote on Network Security Using Cryptographic Techniques

Network Security is the most vital component in information security because it is responsible for securing all information passed through networked computers. Network Security refers to all hardware and software functions, characteristics, features, operational procedures, accountability, measures, access control, and administrative and management policy required to provide an acceptable level of protection for Hardware and Software , and information in a network. Only one particular element underlies many of the security mechanisms in use: Cryptographic techniques; hence our focus is on this area Cryptography.

[3] DECENTRALIZED COMPUTING

Wireless ad-hoc network a decentralized network
A wireless ad-hoc network, also known as IBSS - Independent Basic Service Set, is a computer network in which the communication links are wireless. The network is ad-hoc because each node is willing to forward data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. This is in contrast to older network technologies in which some designated nodes, usually with custom

hardware and variously known as routers, switches, hubs, and firewalls, perform the task of forwarding the data. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts.

The earliest wireless ad-hoc networks were called "packet radio" networks, and were sponsored by Defense Advanced Research Projects Agency (DARPA) in the early 1970s. Bolt, Beranek and Newman Technologies (BBN) and SRI International designed, built, and experimented with these earliest systems. Experimenters included Jerry Burchfield, Robert Kahn, and Ray Tomlinson of later TEN-EXtended (TENEX), Internet and email fame. Similar experiments took place in the Ham radio community. It is interesting to note that these early packet radio systems predated the Internet, and indeed were part of the motivation of the original Internet Protocol suite. Later DARPA experiments included the Survivable Radio Network (SURAN) project, which took place in the 1980s. Another third wave of academic activity started in the mid-1990s with the advent of inexpensive 802.11 radio cards for personal computers. Current wireless ad-hoc networks are designed primarily for military utility.

Application of wireless network

The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes can't be relied on and may improve the scalability of networks compared to wireless managed networks, though theoretical and practical limits to the overall capacity of such networks have been identified. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad hoc networks to be formed quickly. Wireless ad-hoc networks can be further classified by their application:

Distributed Networking is a distributed computing network system, said to be "distributed" when the computer programming and the data to be worked on are spread out over more than one computer. Usually, this is implemented over a network.

Prior to the emergence of low-cost desktop computer power, computing was generally centralized to one computer. Although such centers still exist, distribution networking applications and data operate more efficiently over a mix of desktop workstations, local area network servers, regional servers, Web servers, and other servers.

Distributed computing is a field of computer science that studies distributed systems. A *distributed system* is a software system in which components located on networked computers communicate and coordinate their actions by passing messages. The components interact with each other in order to achieve a common goal. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. Examples of distributed systems vary from SOA-based systems to massively multiplayer online games to peer-to-peer applications.

A computer program that runs in a distributed system is called a **distributed program**, and distributed programming is the process of writing such programs. There are many alternatives for the message passing mechanism, including RPC-like connectors and message queues. An important goal and challenge of distributed systems is location transparency.

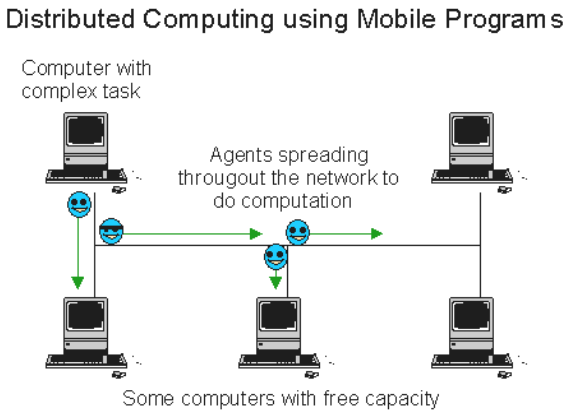

Fig 1: Distributed Computing using Mobile Programs

[4] **Problem statement**

Distributed Network security is sometimes more than what people always thought it to be,malware, virus, Trojan, hackers. Distributed Network security could be caused by unintentional human error and it could be compromised by human nature as well.

A common Distributed network security problem (Employees) most organizations are facing

sometimes has to do with the company's employees and their various errors they make.
According to Dr. Michael E. Whitman, CISM, CISSP, and the author of the
textbook "Principals of Information Security, "Humans make mistakes; sometimes that is due to inexperience or improper training, and sometimes it because an incorrect assumption was reached. But regardless of the reason
— and the lack of malicious intent—something as simple as a keyboarding error has the potential to cause a worldwide Internet outage". (Whitman and Mattord 2012) The problem of piracy is another common network problem
.
Piracy is a situation where intellectual properties are compromised although there are technical mechanisms that aid in enforcing copyright laws to tackle this problem.
However it is not only human errors that can cause problem to network security, problems can also be caused by natural forces like fire breakouts, earthquakes, floods lightning etc.
The ways network administrators think about securing networks has been changed by an increasingly dynamic and technically challenging risk environment.

[5] Security of Distributed network

During this time when the Internet provides essential communication between tens of millions of people and is being increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography. While cryptography is necessary for secure communications, it is not sufficient. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

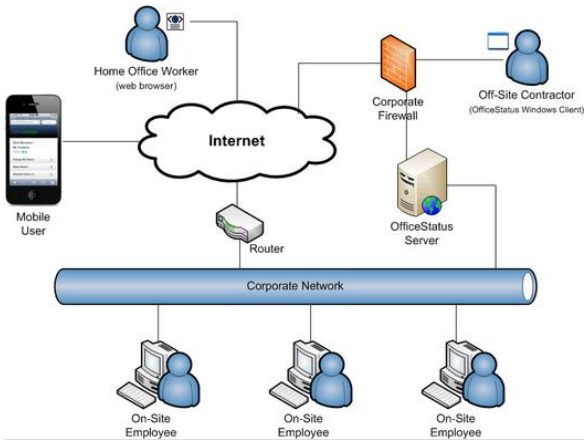

Fig 2: Security of distributed network

Cryptography prior to the modern age was effectively synonymous with encryption, the conversion of information from a readable state to apparent nonsense. The originator of an encrypted message shared the decoding technique needed to recover the original information only with intended recipients, thereby precluding unwanted persons to do the same. Since World War I and the advent of the computer, the methods used to carry out cryptology have become increasingly complex and its application more widespread.

[6] OBJECTIVE OF RESEARCH

1. Implementing centralized computing with Ad hoc networking.
2. Implementing Distributed computing with Ad hoc networking.
3. Make Comparative study of their implementation
4. Discussion of scope of future enhancement
5. Integration of security in Centralized / Distributed computing using various mechanisms such as firewall, cryptographic techniques.

[7] SCOPE OF RESEARCH AND CONCLUSION

Security is a very complex topic. It is very important to build systems and networks in such a way that the user is not constantly remained of the security system around him. Users who find security policies and systems too restrictive will find ways around them. The proposed system is implemented based on threading concepts so it reduces the CPU utilization hence it reduces the time required for the encryption

and decryption. The proposed system is successfully tested on text. As the scale of distributed computing continues to grow, the reliability of the system becomes more crucial and failure prediction and correction mechanisms play a major role in system reliability. The distributed computing is very flexible by reducing workload communicative which enhances human to human communication. We address reliability issue by developing an efficient fault management system for distributed system. Various techniques have been proposed for detecting faults in distributed computing. Once the faults are detected, one may diagnose the system to track the root cause. In this research, the development of distributed systems was discussed in terms of what a distributed system is and the objectives of setting up a distributed system.

From all the available distributed and centralized systems, four most commonly used distributed systems were discussed in depth and then the security issues faced by these systems and the solutions proposed by various researchers were discussed in depth. Finally the security issues and solutions proposed for different systems were summarized and compared with each other. In future the authors are keen to develop the new and competitive approaches for the development of secure distributed systems.

References

[1] Bart Preneel, "The Cryptographers' Track at the RSA conference", 2005, Lecture notes in computer Science3376, springer-Verlag, pp. 29-43, extended version: http://eprint. iacr.org/2004/222/.

[2] Ilango Sriram, "Distributed, Parallel and Cluster computing", 2009, a Simulation Tool Exploring Cloud-Scale Data Centres, In: CloudCom 2009, LNCS 5931, pp. 381-392, 2009

[3] S erotavaGesevone, " Akamai Introduces Cloud-Based Firewall Provides a scalable edge defense system for blocking Web application attacks in the cloud", 2009.
http://cloudcomputing.sys-con.com/node/1219023.

[4] Peter mill and Tim grance, "The NIST Definition of Cloud Computing", 2011, National Institute of Standards and Technology ,Gaitherbsburg,MD 20899-8930, NIST Special Publication 800-145.

[5] Ellen Messmer, "New security demands arising for virtualization, cloud computing", 2011, http://www.networkworld.com/article/2178628/virtualization/gartner--new-security-demands-arising-for-virtualization--cloud-computing.html

[6] Sumedha Kaushik and Ankur Singhal, "Network Security Using Cryptographic Techniques" 2012, volume 2, Issue 12.

[7] Charles Miers, Fernando Redigolo dna Marcos Simplicio ,"A quantitative analysis of current security concerns and solutions for cloud computing " ,2012 ,*Journal of Cloud Computing: Advances, Systems and Applications* doi:10.1186/2192-113X-1-11
The electronic version of this article is the complete one and can be found online at: http://www.journalofcloudcomputing.com/content/1/1/11

[8] Rabi Prasad Padhay, " An Enterprise Cloud Model for Optimizing IT Infrastructure" ,2012 ,International Journal of Cloud Computing and Services Science (IJ-CLOSER) Vol.1, No.3, pp. 123~133 ISSN: 2089-3337 : http://iaesjournal.com/online/index.php/ IJ-CLOSER

[9] Nelson Gonzalez, et. al. ,"A quantitative analysis of current security concerns and solutions for cloud computing " ,2012 ,*Journal of Cloud Computing: Advances, Systems and Applications* doi:10.1186/2192-113X-1-11The electronic version of this article is the complete one and can be found online at: http://www.journalofcloudcomputing.com/ content/1/1/11

[10] CSA "Security Guidance for Critical Areas of Focus in Cloud Computing", (2009), Tech. rep., Cloud Security Alliance.