IJTRET "Voice of Innovative Minds"

doi.org/10.54473/IJTRET.2022.6105
International Journal of Trendy Research in Engineering and Technology
Volume 6 Issue 1 February 2022
ISSN NO 2582-0958

UPDATES ON DEFENSE AND ATTACK ON DISTRIBUTED SYSTEMS

Subramanya.G.Bhagwath,
Dept. of Computer Science & Engineering
Anjuman Institute of Technology and Management , Bhatkal ,India
sgbhagwath@anjuman.edu.in

ABSTRACT

These days, more and more People utilize the internet to access a range of services, while many businesses employ dispersed space to provide services to clients. Distributed computing systems allow the same / different computers and workstations to function as computer hotpots. In this case, operators can have similar access to local and remote resources to run processes. Users are not warned about which PCs their processes are operating on. This can create more or less complex security issues As a result, a distributed safe environment is required in which all operations and operations can be conducted securely.In distributed systems it is very important to provide the service anytime, anywhere to customers, this requires timely management of all computer and communication services, timely allocation of resources and their proper functioning. In a distributed area environmental safety is a major concern. This paper provides security reviews of distributed systems. This begins with a study of the different distributed systems in the literature. Different systems are discussed for the most recent highlights. Finally, various aspects of the safety of distributed systems and significant research tips are explored

Keywords— distributed systems, security issues, grid computing

I. INTRODUCTION

A distributed system in computer science is an unified system of distributed computers, processors or processes that communicate together through common communication medium or network in order to transmit messages. This distribution could be physical (over a geographical area) or logically (over a virtual space).

. Researchers have used a variety of concepts to define what a distributed system is in the literature. "A system in which hardware and software components are installed on a geographically distributed computer that integrates and shares their operations by transferring messages between them," according to Coulouris et al[1]. The distributed system, according to Tanenbaum and Van Steen, is "a collection of programmes that seem to users as a single system" [2]. A distributed system, according to Tanenbaum's definition, refers to a software system rather than the hardware used to create the system. To summarise these definitions, a distributed system is a system that connects with hardware and distributed software in order to accomplish its goals.. together to create a set of related tasks aimed at the same purpose. Many people view a distributed system and a computer network as one. However, these two words imply two distinct, but related, m eanings.

A computer network is a collection of separate computers th at are linked together. Because the computer network does n ot hide the presence of many computers, a user using a com puter network recognises that he or she is using different ap plications on different machines. On the other hand, a distrib uted system creates the idea that the user is working on a sin gle, powerful computer with additional resources. Because the distributed computer operating system can ident ify the necessary machines and perform functions without a ny direct user intervention, the presence of numerous indepe ndent computers is clear to the user [3].

The following are the goals of distributed systems: a. Transparency b. Reliability c. Performance d. Scalability e. Openness System security must be carefully monitored in order to meet the above objectives, as it is one of the fundamental challenges in distributed systems [4]. It should be noted at all stages of distributed system development, including design, implementation, and administration. In this paper, we look at how security is implemented in some of the most extensively used systems, as well as how security problems in a distributed system are handled.

.

II. DISTRIBUTED SYSTEMS

A. *Advantages of Distributed Systems.*

The distributed system has features in the central system such as economy, speed, environmental distribution, and growing growth. In addition, a distributed computer achieves the following benefits [5]:

. Increased Performance: The presence of multiple nodes in a distributed system allows applications to be processed uniformly and thus improve system performance and system performance.

- Service Sharing: Distributed systems enable effective access to different system resources. Users can share special purposes and sometimes expensive hardware and software services such as, database server, compute server, virtual reality server, multimedia information server etc.

• Extended Extensions: Distributed systems are designed to be modular and flexible. For specific statistics, the system will automatically configure it to include a large number of nodes and resources while in some cases,will contain a few resources. In addition, file system capacity and computing power can be increased exponentially. Perhaps the best feature of a distributed system over a central system lies in its modular expansion.

• Increased Reliability, Availability, and Error tolerance: The integration of multiple and final computer resources into distributed systems makes it more attractive and less expensive to introduce malfunctions in order to improve system reliability and error tolerance. The system can tolerate failure in one area by assigning its functions to another available. In addition, due to the increased reliability target embedded within the distributed system. If one machine crashes, the whole system does not crash, unlike the central system [6].

These benefits cannot be easily achieved, since designing a common distributed computer program is a complex process. This process has many challenges that designers have to overcome. In the next section, major challenges of the distributed system are introduced

B. *Challenges of Distributed Systems*

As the scope and scope of distributed programs and applications expand, various challenges may be encountered [1]. In this section, the main challenges are described:

. Heterogeneity: Distributed systems that allow users to access resources and run applications on a separate set of computers and networks. Heterogeneity (i.e., diversity and diversity) applies to all of the following: networks, computer systems, operating systems, programming languages, and the use of different engineers [1].

• Openness: The openness of the computer system is a factor that determines whether the system can be expanded and re-used in a variety of ways. The openness of the distributed system is largely determined by the quality of the new resources sharing services that can be added and made available for use by a variety of client programs. Openness will not be achieved unless specificity and documentation of the main interface of system components are made available to software developers [1].

• Scaling: Distributed systems work efficiently and effectively on many different scales, from small intranet to internet. The number of computers and servers on the Internet has grown significantly. System
is defined as the rate at which it will remain active if there is a significant increase in the number of resources and the number of users.

• Distribution Transparency: Displacement is defined as user encryption and component system divider in distributed system. Thus, the system is seen as a whole rather than as a collection of independent components [1]. The problem with striving for transparency in distribution to very large systems is that performance will drop to an unacceptable level. In addition, network delays have a low natural limitation, when interacting with long-distance communication [7].

• Planning: An organization that is allocated a schedule ignores the central organizational boundaries in terms of tolerance, resilience, and independence. This approach achieves both, a small resource sharing area (e.g. sharing resources under the same administrative domain) in a large area. However, this approach raises significant challenges in the field of distributed information management, enforcement comprehensive system integration, security, app user authentication, and service provider variability [8].

• Security and Trust: Many of the information services made available and stored on distributed systems have a high internal value for their users. Their safety is therefore of paramount importance [1]. An organization subdivided into distributed systems raises significant challenges in the areas of security and trust management. Using a secure distributed system requires potentially effective solutions dealing with various safety issues [8].

.

III. Types

There are many distributed systems running today. In the next section, we present the most widely distributed computer paradigms.

There are many distributed systems running today. Following are some of the most popular distributed systems in use today. Cluster Computing, Grid Computing, distributed storage systems, Distributed Database System.

.

A. *Cluster Computing*

Users can activate and introduce computers connected to high-speed networks as a single computer. A collection is a group of computers that are linked together to form a single resource group. By splitting down all work into smaller independent tasks, every task assigned to the collection will work on all machines in the collection in the same way. The ultimate product would then be formed by combining the effects of small tasks [5].9 Organizations can use cluster computing to boost their processing capability by combining common and widely available technology. These assets, also known as computer programmes and software, can be obtained for a lesser price [10]. Cluster computing has exploded in popularity in recent years.. Collections are used by almost 80% of the world's top 500 universities. Scientific, engineering, commercial, and industrial applications that demand high availability and output output are typically performed on collections [11]. Protein sequence in biological applications, seismic modelling in public engineering, ground source petroleum reservoir simulation, and petroleum engineering [12-15].

B. Grid Compuring

A grid is a distributed computing system that combines a large number of small, tightly connected computers to generate a massive visible supercomputer. This virtual supercomputer must perform incredible feats in order for any single machine to complete them in a timely manner. The grid is characterised as a compact and distributed system that can select, share, and integrate geographically scattered resources based on their availability, power, efficiency, and cost that match the User Service (QoS) criteria over operational time [16]. Grid computing brings together computer resources that are dispersed across a huge number of people and organisations.. The main purpose of the grid system is to work collaboratively across multiple systems to solve a single computer task by breaking down the task into smaller tasks that it contains and distributing those tasks to different computers. The middleware used in grid computing is responsible for classifying and sharing tasks. The size of the grid system can vary from a few hundred computers within an organization to large systems comprising thousands of nodes in multiple organizations. A small grid confined to a single organization is commonly known as an intra-node corporation while a large broad system is called an inter node corporation [17]. Grids used to create scientific, mathematical, and computer-focused study problems by volunteers. Drug detection, economic forecasting, earthquake analysis, and back-end e-commerce office data processing are just a few of the tasks commonly solved using grid computing.

C. Distributed Storage Systems

The rapid growth of storage capacity, bandwidth and computational resources and the reduction in the cost of storage equipment have fueled the popularity of distributed storage systems. The main purpose of distributing storage across multiple devices is to protect the data in the event of a disk failure through mass storage on multiple devices and to make the data available closer to the user in the most widely distributed system [18]. There are four main types of storage systems widely distributed. There are, Server Attached Redundant Array of Independent Disks (RAID), intermediate RAID, Network Attached Storage (NAS) and Local Area Network (SAN). NAS and SAN are the most widely distributed distributed methods in four.
Because of these variances, NAS and SAN have slight discrepancies in approved data transmission mechanisms between devices and activities. The TCP/IP protocol is mostly used by NAS to transport data to numerous devices, whereas SAN employs SCSI settings for fibre channels. As a result, any portable network that supports TCP/IP, such as Ethernet, FDDI, or ATM, can be used with NAS. SAN, on the other hand, can only be utilised for fibre channel. Because TCP has higher overhead and SCSI is quicker than TCP / IP networks, SAN outperforms NAS.

D. Distributed Databasee System

A distributed database system is a collection of standalone web apps dispersed across all computers that share data so that the user can access it from anywhere as if it were stored locally, regardless of where the data is stored.

IV. SECURITY IN DISTRIBUTED SYSTEMS

Security services are generally divided into six categories: Privacy, Data Integrity, Authentication, Authorization, Rejection, and Accountability [6] which will be described below.

• Confidentiality: Important data transferred or transported between parties must be protected and protected. Confidentiality is the concept of ensuring that important data is kept completely disclosed in unauthorized companies [19].
. Data Integrity: Data integrity means maintaining and ensuring the accuracy and consistency of data throughout its life cycle. This means that data cannot be converted without the consent of its official user [20]. That is, it ensures that important data has not been altered or deleted in an unauthorized or unrecognized manner.
• Authentication: Authentication is a basic protection against distributed systems, requiring mutual trust [19]. It is also important that authenticity confirms that both parties are the ones who claim to be. Some information protection systems incorporate authentication features such as “digital signatures”, which provide proof that the message data is authentic and sent by someone with the appropriate signature keys.
• Authorization and Access Control: Authorization management has become one of the most important issues related to distributed programs. It is used to provide a single secure access point that allows users to connect to the network and access authorized services. On the other hand, access control prevents unauthorized people from accessing the system [21].
. Non-refusal: Non-refusal the idea of ensuring that a party to the dispute cannot deny or dispute the validity of the statement. That is, the sender cannot deny sending the message [20].
• Accountability: Although security has been addressed in a number of areas, accountability is one of the key components of non-compliance with modern computer programs [22]. The ability to recognize not only mistakes, but also to find the business / organizations responsible for failure is essential
.

A. SECURITY ATTACKS ON DISTRIBUTED SYSTEMS

Distributed service denials and identity attacks occur mainly on a distributed system [20]. Distributed Denial of Service (DDoS) Attack Denial of service (DoS) is an attack where the main purpose of the attacker or hacker is to destroy the services used by the legitimate user. That is, the attacker is trying to prevent the real user from using the service. When this attack occurs on a distributed system, it is called a Distributed Denial of Service (DDoS) attack. A DDoS attack is when a host of vulnerable programs attack a single target, and triggers a refusal of service for targeted system users. Overcrowding of incoming messages causes the targeted system to shut down, preventing genuine users from accessing the system. An internet hacker begins a conventional DDoS assault by exploiting the vulnerabilities of a single computer system and establishing a DDoS master. The attacker identifies and links to other possibly vulnerable programmes from the main software. Online, there are a plethora of cracked tools available. The attacker can order controlled devices to perform enormous flood attacks against a specific target with a single command [20].

B. Identity Attack on a Distributed System

Identity Attack incorrectly receives authorized input information and uses that information to commit fraud. Many networks and operating systems use the computer's Internet address to identify legitimate business. In some cases, an IP address may be considered spoofing identity. An attacker may use special programs to create IP packets that appear to come from valid addresses within a business intranet. After accessing the network by a valid IP address, the attacker may edit, rewrite, or delete your data. An attacker can also carry out other types of attacks, as described in the following sections. In P2P, identity theft allows malicious peers on the network to shoot application-level applications and take responsibility for any part of the application [23].
As mentioned above, the four distributed systems used are evaluated in terms of the security issues they face and the proposed solution to avoid these problems. The four models are: cluster computing, P2P networks, grid computing, and cloud computing. It is fair to say that collections have laid the necessary foundation for building large grids and clouds. On the other hand, grid / cloud platforms are considered as service providers. In this section, the authors focus on grid and cloud security, as these programs provide a wide range of services and are widely used by various applications. First, a brief study of the compilation and security of P2P will be presented. After that, the authors will present various security issues and solutions for both grid and cloud in detail

C. CLUSTER COMPUTING SECURITY

When computing clusters were made public online, they came under a variety of attacks. The most common types of clutter attacks are computer cycle theft, spying links between nodes, and service interruptions [24]. Collections should therefore be protected by security measures that include services such as, authentication, integrity checking, and confidentiality. The main purpose of security measures is to protect the system from hackers, as well as to meet the security requirements of the applications. It can therefore be seen that computer hackers are vulnerable to malicious attacks, such as hackers and crackers, due to their open nature and use of public resources. Extensive research has been done by several researchers on group safety. Researchers have proposed a number of methods that can be used to protect groups from these attacks [25]. Li and Vaughn learned the dangers of cybersecurity using e-graphs. They emulated several attacks that could be carried on in secrecy, integrity and discovery. Show them that e-graphs can be simplified based on domain information such as setup, and vulnerability. They also say that this process could be used to award collective certificates with the help of a collective risk information base.
[26].
Xie and Qin proposed two resource allocation techniques [24]:
1. Deadline and Security Obstacles TAPADS (Assignment of Functions for Common Requests with Deadline and Security Issues), and
2. SHARP (Short-Handed Assignment of Functions for Common Requests with Deadline and Security Issues) (Allocation of Security Monitoring Services and Heterogeneity-Aware for Parallel jobs).
These two systems ensure that the same applications are made to computer systems that meet security requirements, as well as the deadline [24]. It may therefore be seen that if these systems primarily validate system availability at the time of application, it is an indication of availability.
Denial of Service (DoS) attacks are one of the most common attacks on distributed systems. This attack has targeted resources so much that resources are restricted from performing their official duties. In ref [27], an introduction to the use of resources and the Markova chain to reduce the effects of DoS attacks on a wireless sensor-based network. The Markov series approach was used to determine the likelihood that functional groups would combine to assess survival rates (defined as the ability to provide basic services after an attack or system error) in different regions.
S. Thalod and R. Niwas [28] proposed a security model for computer networks based on the development of cluster computing, using the various tools available in the TCP / IP security model. Each tool has its own security features that make the system secure. They have used these security tools with their security features at various levels of cluster computing architecture, to make the computer system more secure and secure.

D. GRID COMPUTING SECURITY

Grid computer systems provide a few security measures to protect grid resources from attack. Middleware is one of the most important system software in grid infrastructure as it provides standard communication infrastructure and makes grid resources available in applications. Middleware also allows the same security configuration in the service container or message level. Grid verification is based on Critical Public Infrastructure (PKI) and is capable of managing various types of user information such as PKI, SAML, Kerberos tickets, password, etc. The Virtual Organization Membership Service manages authorization for access to grid resources based on the user's Virtual

Organization (VO) attributes (VOMS). The Grid Certification Authority (CA) certificate and other proxy-generated projects are used to maintain trust in grid systems, and the trust relationship is represented by a sequence of certificates. The grid verification module is one of the most important components for preventing illegal access to the internal grid and protecting the grid system from external users. This module deals with security concerns from within the grid, where authorised grid users engage in illicit (unauthorised) actions. Almost every grid system accessible today has one or more of these grid security systems. A few community efforts in the domain of grid middleware interaction are underway, with the goal of eventually including grid security as a single integrated security component and system.

E. *Distributed Storage System Security*

Several practical studies in the area of threat modelling and establishing a security model to defend distributed storage systems are now underway. Data saved on system storage devices is the most valuable resource in a distributed storage system. This information must be appropriately labelled and safeguarded. And any defence system introduced should be backwards compatible, meaning that it should protect not just data kept once the security system is installed, but also data stored prior to the system's launch. Hasan et al. presented the CIAA model, which is a threat model. The Confidentiality, Integrity, Availability, and Verification aspects of security are all addressed in this paradigm. The authors developed this approach by organising risks into a shared storage system under each component of the CIAA security pillars and providing techniques for avoiding threats. The Data Lifecycle Model, which investigates the types of vulnerabilities that might arise at various stages of the data process from creation to extinction, is another security model described by the authors. Threats are divided into six categories in this approach, and solutions are offered Dikaliotis, Dimakis, and Ho devised a simple linear speed detection system for detecting mistakes in archived storage systems. MCR (Mutually Cooperative Recovery) allows the system to recover data in the event of multiple node failures. The construction of a network coding system based on (n, k) stiff MDS code can aid in the restoration of systems that have experienced a relatively minor failure [18]. As a result, it's clear that security strategies in distributed storage systems are more concerned with data integrity and failure management (availability).

F. *Distributed Database Security*

When compared to centralised online systems, distributed database systems suffer additional security vulnerabilities. The advent of numerous new website models, such as object-based website model, temporary website model, object-related data model, and so on, has substantially hampered improving the security of distributed website systems. In a typical security approach, all data on a website and people that access it have the same level of security. A secure multi-level secure system ensures that each transaction and piece of data is kept safe. The level of security supplied represents the level of performance, and the level of data separation is represented by the level of separationA high-level secure web-based management system (MLS / DBMS) restricts a site's performance based on security requirements. It can be observed from the previous explanation that by separating military information, the security of limiting access to disseminated information can be improved. Zubi presented a concept that might improve the scalability, accessibility, and flexibility of a distributed data system while accessing a wide range of data. To maintain the security of the dispersed information system, he also recommended multi-level access control, confidentiality, reliability and integrity.

CONCLUSION

As can be seen from the foregoing discussion, security is critical when systems are deployed across numerous locations. The security requirements for each type of distributed system are different. However, the CIA trinity is at the centre of every security implementation in every programme. Data transfer and access to distant resources are the primary concerns for computer collections and grids. Due to the similar nature of clusters, security is a little easier in comparison to the grid. The Denial of Service (DoS) attack is one of the most common attacks on clusters. To mitigate the impact of DoS assaults, researchers have proposed novel solutions based on the markov series. Grid The grid system's middleware layer provides a secure platform for grid users. The grid system employs X.509 certificates and PKI-based security. The grid's user verification module protects against threats from outside sources as well as illicit behaviours by internal users. Data acquisition is crucial to the security of distributed storage systems. Data protection and data protection in the event of node failure are two of the most important aspects of distributed storage. To safeguard the final system from assault and node failure, researchers have proposed a variety of concepts and approaches. The availability of several types of website models has made the use of security more complex in the distributed website system. However, researchers have demonstrated that distributed data security may be improved by employing multi-level security based on the separation of military intelligence and access control. The development of distributed systems was covered in this study in terms of what a distributed system is and the goals of constructing one. The four most commonly distributed applications were selected among all accessible distributed programmes, and the security challenges they face, as well as the solutions suggested by various researchers, were thoroughly explored. Finally, the security concerns and solutions provided for the various systems were summarised and contrasted. In this study, each security feature is discussed separately, such as information security, physical security, and network technical security. In a distributed environment, all of these securities should be used

appropriately. The tactics for exploiting these securities are discussed in this paper. Two DDoS attacks and an Identity Attack are also described in this study. This type of assault can happen in a distributed system and has happened before. The answer to this attack is discussed in this publication.
After learning all of this, the norm is to make the distributed system more adaptable and dynamic.

References

[1] G. F. Coulouris, J. Dollimore, and T. Kindberg, Distributed Systems-Concepts and Design, 4th ed. London, England: Addison - Wesley, 2005.

[2] T. S. Andrew and M. V. Steen, Distributed Systems: Principles and Paradigms, 2nd ed. Upper Saddle River, NJ, USA: Pearson Higher Education, 2007.

[3] K. Nadiminti, M. D. De Assunçao, and R. Buyya, “Distributed systems and recent innovations: Challenges and benefits,” InfoNet Magazine, vol. 16, no. 3, September 2006.

[4] Z. Shen and X. Wu, "The protection for private keys in distributed computing system enabled by trusted computing platform," in Proc. 2010 IEEE International Conference on Computer Design and Applications, vol. 5, 2010, pp. 576-580

[5]Srinivasa, K., & Muppalla, A. (2015). Guide to high performance distributed computing: case studies with hadoop. Scalding and Spark, Springer International Publishing. doi:10.1007/978-3-319-13497-0

[6]Alotaibi, S., Wald, M., & Argles, D. (2010). Using fingerprint recognition in a new security model for accessing distributed systems. International Journal of IntelligentComputing Research, 1(4), 194–203.

[7]Steen, M., Pierre, G., & Voulgaris, S. (2012). Challenges in very large distributed systems. Journal of Internet Services and Applications, (3), 59-66.

[8]Rahman, M., Ranjan, R., & Buyya, R. (2012). Decentralization in distributed systems: Challenges, technologies, and opportunities.

.[9]Y. Amir, Y. Kim, C. Nita-Rotaru, J. L. Schultz, J. Stanton, and G. Tsudik, “Secure group communication using robust contributory key agreement,” IEEE Transactions on Parallel and Distributed Systems, vol. 15, no. 5, pp. 468-480, 2004.

[10]S. Lakshmanan, M. Ahamad, and H. Venkateswaran, "Responsive security for stored data," IEEE Transactions on Parallel and Distributed Systems, vol. 14, no. 9, pp. 818-828, 2003.

[11]Physical Security in Distributed IT Environments. [Online]. Available: http://www.ithandbook.ffiec.gov

[12]“Packet Filtering” Chapter 6. [Online]. Available: http://www.diablotin.com/librarie/networking/firewall/ch06_01.ht m

[13] L. L. Peterson and B. S. Davie, “Computer network “ (2009 edition, page no 626 and 627)

[14]G. Misherghi, L. Yuan, Z. Su, C. N. Chuah, and H. Chen, "A general framework for benchmarking firewall optimization techniques," IEEE Transactions on Network and Service Management, vol. 5, no. 4, pp. 227-238, 2008.

[15]Emir Accilien CMPT 585 001. Security issues in Distributed Systems:Is Kerberos the Answer? [Online]. Available: http://www.pages.csam.montclair.edu

[16]A. Saafan. (23 March 2009). Distributed Denial of Service Attacks: Explain nation, classification and suggested Solutions. [Online]. Available: http://www.exploit-db.com

[17]K. P. Puttaswamy, H. Zheng, and B. Y. Zhao, "Securing structured overlays against identity attacks," IEEE Transactions on Parallel and Distributed Systems, vol. 20, no. 10, pp. 1487-1498, 2009.

[18]D. Harinath, et al. “Enhancing security using video steganography and water marking,” Advances in Image and Video Processing, [S.l.], v. 3, n. 5, p. 1, nov. 2015. Available at: <http://scholarpublishing.org/index.php/AIVP/article/view/1650/8 87>. Date accessed: 16 Nov. 2015. doi:http://dx.doi.org/10.14738/aivp.35.1650.

[19]Abbas, A., & Khan, S. (2014). A review on the state-of-the-art: Privacy preservingapproaches in e-Health clouds. IEEE Journal Biomedical Health Information, 18(4),1431 – 1441. doi:10.1109/JBHI.2014.2300846 PMID:25014943

[20]Kumar, M., & Agrawal, N. (2013). Analysis of different security issues and attacks in distributed system: A-review. International Journal of Advanced Research in Computer Science and Software Engineering, 3(4), 232 –237.

[21]Koshutanski, H. (2009). A Survey on distributed access control systems for web business processes. International Journal of Network Security, 9(1), 61–69.

[22]Karajeh, H., Maqableh, M., & Masa’deh, R. (2011). Security of cloud computing environment. In Proceedings of the 23rd IBIMA Conference on Vision 2020: Sustainable Growth, Economic Development, and Global Competitiveness

[23]Puttaswamy, K., Zheng, H., & Zhao, B. (2009). Securing structured overlays against identity attacks. IEEE Transactions on Parallel and Distributed Systems, 20(10), 1487–1498. doi:10.1109/TPDS.2008.241

[24]Xie, T., & Qin, X. (2008). Security-aware resource allocation for real-time paralleljobs on homogeneous and heterogeneous clusters. IEEE Transactions on Paralleland Distributed Systems, 19(5), 682 – 697. doi:10.1109/TPDS.2007.70776

[25]Firdhous, M. (2011). Implementation of security in distributed systems – A comparative study.

International Journal of Computer Information Systems, 2(2), 1‐6.

[26]Li, W., & Vaughn, R. (2006). Cluster security research involving the modeling of network exploitations using exploitation graphs. In Proceedings of the 6th IEEE International Symposium on Cluster Computing and the Grid Workshop(pp.26-36). doi:10.1109/CCGRID.2006.1630921

[27]Zhongqiu, J., Shu, Y., & Liangmin, W. (2009). Survivability evaluation of clusterbased wireless sensor network under DoS attacks. In Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing, (WiCom '09) (pp. 1-4).

[28]Thalod, S., & Niwas, R. (2013). Security model for computer network based oncluster computing. International Journal of Engineering and Computer Science,2(6), 1920‐1927.