IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Recovery and Security in Distributed System

Ms. Gurpreet Kaur Sodhi

Assistant Professor, University Institute of Computing (UIC), Chandigarh University, Gharaun, Mohali, India

Abstract: Distributed systems have immense practical value in our computerized world and have many applications, including scientific, engineering, commercial and industrial. However, by their very nature of interconnectedness, distributed systems are subject to security issues and failures. These issues must be adequately addressed through effective techniques and methods to correct these problems.

Keywords: Distributed systems, Security, Failures, Recovery.

I. INTRODUCTION

As technology advances our world becomes smaller and more connected and nowhere is this more evident than with computer-related technology. We live in an interconnected world, a networked world, and in this climate computers rarely work in isolation. Computers collaborate with each other for many purposes, including communication, processing, data transfer and storage. Systems that work in this collaborative manner and that are scattered over large distances are called distributed systems [1]. These systems have become ubiquitous in our modern world and have numerous applications, including search, entertainment and e-commerce, among others [2]. Distributed systems are immensely practical; however, along with their many benefits are some recurring issues such as security and recovery of failed systems.

II.OBJECTIVES

The objectives of this short paper are to define what is meant by distributed systems and to briefly look at the issues of security and recovery affecting these systems.

III.RESEARCH METHODOLOGY

Research methodology consisted of an Internet search for several research papers on the issues of security and recovery in distributed systems.

IV.IMPLICATIONS AND CONTRIBUTIONS

Distributed systems are of great value; yet, by their very nature, they are subject to various types of attacks. These systems communicate with dispersed hardware and software to coordinate the actions of multiple processes running on different autonomous computers so that, together, the various components work together to perform a set of related tasks to achieve a common objective [1].

This results in users feeling like they are working on a single, powerful computer, although, in reality, the system is made up of many different components. Like anything, the more working parts the more potential problems and, in the case of distributed systems, these problems take the nature of outside attacks. Thus, security of distributed systems is a fundamental issue [1].

There are different types of distributed systems and the most popular is what is called cluster computing. This type of system is composed of a set of computers grouped together and communicating over a high speed network. Cluster distributed systems are used to run scientific, engineering, commercial and industrial applications that require high throughput processing [1].

These systems, when made available to the public, can be subject to various types of attacks, including computation-cycle stealing, inter-node communication snooping, and cluster service disruption. Various security mechanisms have thus been formulated to protect the security of these systems from hackers, including authentication, integrity check and confidentiality [1].

In addition to security issues, much attention in distributed systems has been paid to failures of the systems and their recovery. Failures in distributed systems are often unpredictable and can have a wide variety of consequences. Failures result in downtime of the systems which can have significant impacts on the systems' users [3].

Furthermore, failure in one part of a system can negatively affect other parts of the system, resulting in a ripple effect [3]. Before recovery actions can occur, it must first be determined which components in the system have failed, a process which can be very difficult, as is the determination of which sequence of actions to take that would allow the quickest recovery [2]. To ensure optimal efficiency of distributed systems, failures must be quickly detected, effectively diagnosed, and then steps must be taken to correct these failures, while, at the same time, taking into account the possibility of further, related failures [3].

V. CONCLUSION

Computers, in general, have greatly enhanced our world and distributed systems are responsible for a large part of the role that computers play in our lives. Distributed systems have a high practical importance, yet the nature of their success, their interconnectedness, also makes them vulnerable to outside attacks from hackers. In addition, failures in any part of the system can have serious, extensive effects on entire system or, at least, on a major part of it.

Therefore, it is crucial that effective techniques be developed to combat security issues and to effect recovery of failed systems in the quickest manner possible.

REFERENCES

[1] M. Firdhous, "Implementation of Security in Distributed Systems – A Comparative Study," International Journal of Computer Information Systems, vol. 2, no. 2, pp. 1-6, 2011.

[2] K. R. Joshi, M. A. Hiltunen, W. H. Sanders, and R. D. Schlichting, "Probalistic Model-Driven Recovery in Distributed Systems," Transactions on Dependable and Secure Computing, vol. 8, no. 6, pps. 913-928, November/December 2011.

[3] N. Arshad, "A Planning-Based Approach to Failure Recovery in Distributed Systems," PhD theses, Dept. of Computer Science, U. of Colorado, Boulder, CO, 2006.