www.ijemr.net ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962

Volume-5, Issue-3, June-2015

International Journal of Engineering and Management Research

Page Number: 43-45

Autonomic Computing and Its Vision as Future Computing

Vivekananth.P
Senior Lecturer, Computer Science, Sokoto State University, Sokoto, NIGERIA

ABSTRACT

Autonomic computing systems are self-managed systems without the need of human intervention. It is an analogy of the autonomic nervous system in nature. In an autonomic computing system the human operator takes a new rule, instead of controlling the system he just guides the system and devises rules for self-managing system. Every aspect of human life is automated and this makes everyday tasks much easier, so autonomic computing makes all aspect of computing faster and more efficient. The biggest advantage of autonomic computing is it will reduce the need for day to day repetitive administrative tasks and which is the biggest time saver. The four aspects of self-management such as self-configuration, self-protection, -healing are discussed. The need for developing algorithms that is set of rules that can take information and improvise, also the need for design of architecture that provide consistent interfaces and point of control in a heterogeneous environment are also discussed. The paper also analyzes how autonomic communications will be a driving factor for the future internet.

Keywords*----* Autonomic behavior, Self-configuration, Self-healing, Self-management, Self-optimization, Self-protection.

I. INTRODUCTION

Computer application developers and engineers have been working on ways of increasing autonomic capabilities of computers, making them less dependent on people for tasks involving sustaining the efficacy and operation-ability of the system. Such computer attribute is termed autonomic computing, and it entails aspects of self-management such as self-healing, self-protecting, self-optimization and self-configuration. By integrating such attributes to the computer, programs developers and engineers intend to mimic the functions of the autonomic nervous system of animals, particularly humans. Therefore, in order to understand how autonomic computers would work, one needs to have deep insight into how autonomic system in the human body functions to achieve self-configuration, self-healing, self-optimization and self-protection capability.

II. THE GENERAL AUTONOMIC COMPETENCE

Currently, the tendency to assemble heterogeneous components into a meaningful collaborating and profitable system unfortunately leads to deficient security, maintenance needs, and dependability among others. Such obstacles inspired visions of self-aware systems posited in multiple research reports. Most prominently, the IBM's *autonomic computing* vision described by Kephart and Chess [1], gave a detailed description of this phenomena. The label autonomic computing originates from the research on the natural autonomic nervous system. Autonomic computing involves attempting to align to the concept of decoupling the utmost reasoning competence from an underlying, independent maintenance system [2]. In particular, the research centers on potential answers to autonomous maintenance in modern computing infrastructures.

Amid significant researches about self-managing competence of autonomic computing, a common underlying idea is "introducing an autonomous behavior to handle an otherwise complex and unmaintainable system" [2]. In practice, autonomous behavior entails autonomic computers being capable of independently taking steps at runtime and managing the consigned system. Despite such management tasks as configuring, recovering, and adapting being goal dependent, they must produce a consistent system. Importantly, accurate system knowledge enhances the success of a sufficient autonomous behavior. While the research of both the self-adaptive and autonomic computing system [3] [4] align, just the knowledge of external circumstance (context aware) and internal state

(self-aware) enables proper adaptation. Thus, computer system gain such integrated awareness through filtered data related to sensing, and feedback related to effecting interfaces matched with the context culminating in a system review that is accurate [2]. Notably, to maintain a current view and satisfy conditional time limits, the computer system assumes a closed loop system (see fig. 1) [2].

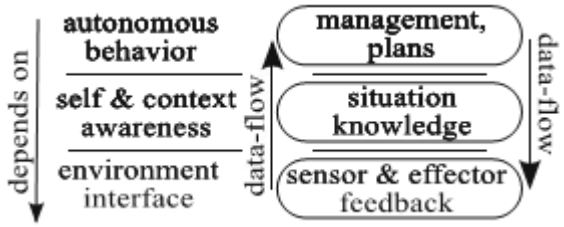

Figure 1: Essential dependencies and data-flow for autonomic computing systems

III. SELF-CONFIGURATION CAPABILITY

Advent of network services represents a principle aspect of the modern network infrastructure [5]. Specifically, in such network environments, servers disperse information about network services configuration among multiple information storages. Usually, the correlation between the storage and use of such configuration information is managed via drivers, processes, or protocols uniquely made for different environment of use. Worth noting, with the expansion in end-user systems integrating into the network concurrent with the number and types of network services, the demand for and complexity of an effective way for managing the correlation between configuration information and its consumption increases.

Self-configuration relates especially to network services, where it refers to the system's ability to configure – set up- its network- its network-based applications and services, consistent to the user's needs and the system's environment. Practically, the system on the side of the user would detect the change in the needs of both the system's environment and the end-user, interpret its impact, and reconfigure itself accordingly. However, the requisite for different rates of disseminating information about altered configuration throughout the system's environment, the variety of system administrator's roles, and the location flexibility complicate the process of configuration behavior of network services that are autonomous [5].

IV. SELF-HEALING COMPETENCE

Studies on self-healing competence of computer originated from self-stabilizing and fault-tolerant systems studies [2]. Fault tolerant systems address characteristic mask permanent and transient system failures to return to a usable state [6]. On the other hand, self-stabilizing systems represent a non-fault masking technique for systems that are tolerant to faults. Such systems have two different attributes described as *convergence* and [7]. Distinctively, convergence refers to the attempts of a system to revert to a legal state in predetermined time regardless of disruptions, while closure refers to the attempts of a system to maintain the previous valid state [7].

Concisely, a computer system with self-healing competence is one that combines survivable system, self-stabilizing, and fault-tolerant capabilities. Consequently, "… a self-healing system should recover from the abnormal (or "unhealthy") state and return to the normative ("healthy") state, and function as it was prior to disruption" [8]. Noteworthy, self-healing systems in a distinct situation act as adjuvants to fault-tolerant systems [8]. Singly, by containing failing parts and securing specific principle services that represent a minimal albeit running system configuration, survivable systems correct malicious behavior. The operation mode of self-healing software is a systematic procedure of identifying and isolating and taking a faulty entity off line, repairing the failed entity, and reinitiating the fixed or replacement entity into the system without distorting its operation [9]. Specifically, the goal of self-healing is to facilitate the reliability of a system by limiting the outages. Therefore, effective self-healing systems can anticipate conflicts in order to avert possible failures.

V. SELF-PROTECTING COMPETENCE

A self-protecting system denotes one which can identify and protect its resources from both internal and external invasions [10]. Typically, such a system aids in detecting hostile behavior and executing autonomous processes to protect itself from invasive behaviors [10]. Unlike self-healing competence, the principle objective of self-protecting systems is to safeguard the environment in which the system runs from malicious, deliberate behaviors. To accomplish this role, a self-protecting system scans the suspicious tasks and responds appropriately without disclosing to the user of the protection process it executes [11]. Practically, a self-protecting system must be able to determine intrusion by differentiating legal from illegal activities. Also, it must have the capacity to respond to invasions, besides having the capability to protect its self-protection entities from disruption [10].

VI. SELF-OPTIMIZATION COMPETENCE

The self-optimization capability is particularly relevant in telecommunication networks, as the recent evolutions of telecommunication networks primarily underscore the need for optimization of network capabilities. In this light, operators confront the problem of containing the costs of their operation besides the challenge of adapting to next-generation services [12]. Because of the ongoing evolution in the profile of service or traffic, an increasing level of complexity and dynamicity, and an extra scaling in size will characterize prospect wired networks; hence, necessitating consistent adjusting of network configuration. A majority of autonomic computing experts believe that self-management, especially self-optimizing competence, provides the accurate framework to solve such network operation challenges.

In the context of networking, optimization challenges share the goal of efficiency versus scalability and dynamicity. Consequently, self-optimization algorithms seem an innovative means to resolve such issues [12]. Moreover, self-optimization requires embedding algorithms that forces decisions, the closest possible, to the functional component. Often, the system determines the limit to closeness from the necessary information for decision-making [12].

VII. CONCLUSION

Autonomic computing offers a range of promise to internet providers. Specifically, autonomic computing would reduce operation costs for the service because fewer personnel would be needed to facilitate its operation. The capacity of autonomic systems to self-manage eliminates the need for human operators. Distinctively, the ability to self-configure will allow internet system to configure effectively its network-based apps and services towards the needs of both the system's current environment and the user. Such capability will fill the gap related to increasing complexity and need for better technique for coordinating the information on configuration needs of the user and system's environment, and its consumption. Self-healing capability will enhance internet reliability by minimizing outages, and self-protecting competence will protect the internet system environment from malware and attacks. Lastly, self-optimization will enable internet to overcome the challenges related to increased complexity and dynamicity, which often compromise its efficiency. Indeed, autonomic computing promises a lot to internet providers.

REFERENCES

[1] O. Jeffrey Kephart, David Chess, The vision of autonomic computing. Computer IEEE Computer Society Press, 36(1), 41–50, 2003.
[2] H. Psaier, S. Dustdar, A survey on self-healing systems: approaches and systems, Computing, 91(1), 43-73, 2011.
[3] M. Salehie, L. Tahvildari, Self-adaptive software: landscape and research challenges, ACM Trans Autonomic Adaptive System, 4(2), 1–42, 2009.
[4] R. Sterritt, Autonomic computing, Innovative System Software Engineering, 1(1), 79–88, 2005.
[5] Brian Melcher, Bradley Mitchell, Towards an autonomic framework: self-configuring network services and developing autonomic applications, Intel Technology Journal, 8(4), 279-290, 2004.
[6] W. Pierce, Failure-tolerant computer design. New York: Academic Press, 1965.
[7] A Arora, M Gouda, Closure and convergence: a foundation of fault-tolerant computing, IEEE Trans Softw Eng, 19(11), 1015–1027, 1993.
[8] D. Ghosh, R. Sharman, H Raghav Rao, S. Upadhyaya, Self-healing systems—survey and synthesis. Decision Support System, 42(4), 2164–2185, 2007.
[9] A. Ganek, T Corbi, The dawning of the autonomic computing era, IBM System Journal, 42(1), 5–18, 2003.
[10] I. Chopra, M. Singh, SHAPE-an approach for self-healing and self-protection in complex distributed networks, Journal of Supercomputing, 67(2), 585-613, 2014.
[11] B. Claudel, N. De Palma, R. Lachaize D. Hagimont, Self-protection for distributed component based applications. Berlin: Springer, 2006.
[12] G. Carofiglio, P. Peloso, H. Pouyllau, Realizing self-management via self-optimization in dynamic networks: Two examples of dynamic resource allocation. Bell Labs Technical Journal (John Wiley & Sons, Inc.), 15(3), 177-192, 2010.