Computers in Industry 99 (2018) 156–172

Contents lists available at ScienceDirect

Computers in Industry

journal homepage: www.elsevier.com/locate/compind

Fault tolerance in cloud computing environment: A systematic survey

Moin Hasan*, Major Singh Goraya

Department of Computer Science and Engineering, Sant Longowal Institute of Engineering and Technology, India

ARTICLE INFO

Keywords:
Cloud computing
Faults and failures
Fault tolerance
Survey

ABSTRACT

Fault tolerance is among the most imperative issues in cloud to deliver reliable services. It is difficult to implement due to dynamic service infrastructure, complex configurations and various interdependencies existing in cloud. Extensive research efforts are consistently being made to implement the fault tolerance in cloud. Implementation of a fault tolerance policy in cloud not only needs specific knowledge of its application domain, but a comprehensive analysis of the background and various prevalent techniques also. Some recent surveys try to assimilate the various fault tolerance architectures and approaches proposed for cloud environment but seem to be limited on some accounts. This paper gives a systematic and comprehensive elucidation of different fault types, their causes and various fault tolerance approaches used in cloud. The paper presents a broad survey of various fault tolerance frameworks in the context of their basic approaches, fault applicability, and other key features. A comparative analysis of the surveyed frameworks is also included in the paper. For the first time, on the basis of an analysis of various fault tolerance frameworks cited in the present paper as well as included in the recently published prime surveys, a quantified view on their applicability is presented. It is observed that primarily the checkpoint-restart and replication oriented fault tolerance techniques are used to target the crash faults in cloud.

1. Introduction

Cloud computing has been prominently existing as an on-demand computing service paradigm and immensely benefiting the small-scale users as well as large-scale commercial and scientific applications. It is defined as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1]. On-demand access, resource autonomy, rapid elasticity and always-on availability are the primary characteristics of cloud computing [2]. Cloud resources are provisioned using standard protocols (IAM, OAuth, OpenID, etc. for authentication; and AMI, OVF, SOAP, REST, etc. for data and workload migration [3]) to create the wider acceptability of cloud services. Besides this, cloud offers greater business agility at the reduced cost which further attracts a vast user base. A recent survey conducted over 433 enterprise respondents containing 1000+ employees reveals that 95% of the respondents are using cloud [4]. Kazarian et al. [5] reported 91% adoption of cloud by the IT professionals in more than 3000 small and midsize businesses. Anticipating its vast benefits, distinguished IT organizations (such as Amazon, Microsoft, IBM, Google, Yahoo, etc.) are into the foray to deliver cloud services.

Though, cloud has gathered much attention over the time, but it is still considered adolescent in terms of fault handling capability [6]. The cloud computing architecture is dynamic and growing in complexity [7–9]. Its deployment uses millions of commodity components rather than conventional ones [10]. Due to this, it is always prone to faults and failures. Fault is an abnormal condition or defect in one or many parts of a system, which may result in the inability of the system to perform its intended functions [11]. Fault occurrence creates error in the system. Error is defined as a deterioration in one or more system components and creates difference between normal and actual state of the system [12]. The errors lead the system to failure, which interrupts the normal delivery of the services and degrades the system performance. Improper handling of system failures may lead the system to an unworkable state [11]. The effects are so adverse at times that they could traumatize the economic state of the service provider. For instance, in 2013, a breakdown of just about 45 min resulted in an economic loss of $5 million to Amazon cloud [13]. It may be one of the reasons for the reluctance of a big pool of users towards acquiring cloud services and makes fault tolerance as one of the most imperative issues in cloud computing.

Fault tolerance is defined as the capability of a system to keep performing its intended task even in the presence of faults [14,15]. Without fault tolerance capability, even a well-designed system with best of the

* Corresponding author.
E-mail addresses: mmoinhhasan@gmail.com (M. Hasan), mjrsingh@yahoo.com (M.S. Goraya).

https://doi.org/10.1016/j.compind.2018.03.027
Received 14 July 2017; Received in revised form 16 January 2018; Accepted 20 March 2018

components and services cannot be considered as reliable [16]. Reliability is a highly significant facet of cloud, as a large number of delay sensitive (real-time) applications are to be executed. Moreover, service reliability is imperative to the wider acceptability of cloud. Therefore, the issue of fault tolerance has got a considerable attention in research and numerous fault tolerance frameworks have been proposed in literature over the period. Through this paper, we endeavour to present a survey of fault tolerance in the cloud computing environment.

1.1. Motivation of the survey

In the literature, we observe that despite extensive research in the field of fault tolerance in cloud, only a few surveys [17–19,16,20,21] have been published. Although, these surveys have considerable contribution in the field, but in themselves, do not seem to be exhaustive and comprehensive. These surveys appear to be limited in respect of one or other account.

Cheraghlou et al. [16] gave only a brief description of different fault tolerance techniques without focusing on fault types. Further, the discussion of only a few number of frameworks in the survey limits its scope. [21] focused directly on fault tolerance and classified fault tolerance policies as *exclusively handled* and *collaboratively handled*. This survey does not provide view on the conventional classification of the fault tolerance models in cloud. Agarwal and Sharma [17] gave the taxonomies of fault, error and failure; but missed the theoretical explanation. The authors have not included any existing fault tolerance framework in the survey to strengthen the discussion of fault tolerance techniques. Ataallah et al. [19] included a brief description of various fault tolerance parameters in their survey, but failed to include the description of fault types. Very limited frameworks have been explained in this survey which are insufficient to describe the state-of-the-art. Several types of faults and fault tolerance techniques are briefly described in the survey given by Saikia and Devi [20]. However, authors have not given any classification of the described faults and fault tolerance techniques in the survey. Further, only a few fault tolerance frameworks are included in the survey without citing any comparative analysis. Amin et al. [18] also enlisted various fault tolerance metrics along with a brief description about fault detection. Again, very limited fault tolerance frameworks are explained without any reflection of the methodology of fault tolerance used in the frameworks.

It can apparently be concluded that none of the above cited surveys presents the complete structure of fault tolerance in cloud computing. In order to understand the complete structure of fault tolerance the readers have to refer different sources. Therefore, we motivated to write a comprehensive and systematic survey on fault tolerance in cloud by describing its complete structure which includes the description of (a) various fault types, their causes and classification; (b) fault tolerance approaches and techniques; and (c) fault tolerance frameworks. Table 1. summarises and present a comparative analysis of the existing surveys cited in this paper and the present survey in the context of inclusion (✓) and non-inclusion (×) of the attributes: fault taxonomy, fault tolerance approaches, fault tolerance frameworks, comparative analysis, and graphical representation.

1.2. Scope of the survey

Scope of the present survey is:

- Description of various fault types and their causes in cloud computing environment.
- Description of basic fault tolerance approaches used in cloud computing environment.
- Description of different fault tolerance frameworks proposed in literature for cloud computing environment.

Fault types are explained in a tabular form for the ease of understanding. A comparative analysis of the surveyed frameworks is also given which focuses on the basic approach, methodologies used, fault applicability and key features.

1.3. Survey plan and organization

The survey plan broadly includes article selection, fault classification, identification of fault tolerance approaches and methods, description of fault tolerance frameworks, discussion and future directions. The survey plan is executed through multiple phases described as follows:

- *Phase-1 (Articles Selection)*: In the first phase number of research articles (including surveys) related to the field are collected from reputed sources. The collected articles are carefully examined and filtered based on their *titles*, *abstracts*, and *research contributions*. While examining the research contributions, the novelty and quality of the work is critically analysed. The articles (regarding each fault tolerance method) for inclusion in the paper are selected with the criteria that the reader would be able to know the basic implementations and possible modifications/customization of each fault tolerance method. Necessary efforts are made to assure and maintain the diversity of the articles in order to remove the ambiguity and enhance the knowledge base of the readers.
- *Phase 2 (Fault Classifications in Cloud)*: In the second phase, the collected articles are intensely scrutinized to identify different fault types in cloud. The identified fault types are thoroughly analysed for their categorization. Section 2 includes the brief description of different fault types, their root causes, and classification in cloud.
- *Phase 3 (Fault Tolerance Approaches in Cloud)*: In this phase, the collected articles are further analysed to identify various fault tolerance approaches in cloud. The identified approaches are enlisted and described in Section 3 of the survey. The fault tolerance methods based on the identified approaches are also explained and hierarchically presented in Section 3.
- *Phase 4 (Fault Tolerance Frameworks in Cloud)*: This phase contains the core research contribution of this survey to explain various fault tolerance frameworks proposed in the literature. The objective is to provide an evolutionary knowledge base in such a way that the research contribution towards each fault tolerance method could be covered. Section 4 explains various prominent fault tolerance

Table 1
Comparison of the present survey with the cited surveys.

Survey Paper	Fault Taxonomy	Fault Tolerance Approaches	Fault Tolerance Frameworks	Comparative Analysis of Frameworks	Graphical Representation of Results
Cheraghlou et al [16]	×	✓	✓	✓	×
Tchana et al. [21]	×	✓	✓	×	✓
Agarwal and Sharma [17]	✓	✓	×	×	×
Ataallah et al.[19]	×	✓	✓	✓	×
Saikia and Devi [20]	✓	×	✓	×	×
Amin et al. [18]	×	✓	✓	×	×
Present Survey	✓	✓	✓	✓	✓