VIETNAM NATIONAL UNIVERSITY-HCMC
Ho Chi Minh University of Technology

SOCIALIST REPUBLIC OF VIETNAM
Independence – Freedom-Happiness

THESIS INFORMATION

Title:	**FAULT DETECTION AND TOLERANT IN CLOUD COMPUTING INFRASTRUCTURE**
Major:	**COMPUTER SCIENCE**
Major code:	**62.48.01.01**
PhD. candidate:	**BUI THANH KHIET**
Suppervisors:	**Assoc. Prof. TRAN CONG HUNG, PhD** **Assoc. Prof. PHAM TRAN VU, PhD**
University:	**HO CHI MINH UNIVERSITY OF TECHNOLOGY (HCMUT), VIETNAM NATIONAL UNIVERSITY (VNU-HCM)**

1. Summary

Cloud computing infrastructure services bring practical convenience, help users to deploy applications flexibly, simplify the rental process, and release resources while renting resources calculated based on use-pay-as-you-go. However, faults on the cloud infrastructure service are unavoidable because of the large scale and network system of the cloud data center along with the complex architecture of thousands of physical servers with different reliability. With the openness, flexibility and complex structure of cloud computing, it leads to many different types of faults from the infrastructure system, the platform to the application. Faults can occur at any particular layer of the cloud and it will affect above layers. If the fault occurs in the operating system of the platform service layer, it can lead to applications on software services to fail. If a fault occurs in the hardware of physical servers, it will affect the infrastructure service layer and continues to lead to the failure in the operating system of the platform service layer, continues to affect the infrastructure service layer, and then software service layer application failures. It can be seen that faults in infrastructure services, especially hardware, will affect and cause great damage to the system. It is imperative to detect typical hardware faults and develop corresponding fault toletrance techniques. Accordingly, cloud computing needs to be able to identify and behave appropriately to ensure transparency, quality of service, and avoid data loss even when faults occur. This ability is known as fault tolerance on cloud infrastructure.

Existing fault tolerance (FT) approaches can be classified into two basic categories, viz. reactive and proactive approaches. The reactive FT approaches handle the faults after their appearance through using system maintenance programs. They are built on responsiveness rather than predictability. They are also conservative by nature, so there's no need to inspect the system's

behavior. As a result, they do not have any unnecessary overhead. Proactive FT approaches, on the other hand, are described as the capacity of the system to be in an active state to avoid potential faults/errors/failures before they occur. Statistics, machine learning, and artificial intelligence approaches are used to continually monitor the system's health and anticipate the likelihood of a fault occurring. The system handles fault occurrence by taking essential actions. A FT approach is an incorporated action of fault detection and fault recovery (reactive FT approach) or fault forecasting and fault prevention (proactive FT approach). Although reactive FT frameworks are popular among researchers till now, the scope of research in proactive FT frameworks is increasing because of ongoing advancements in machine learning and artificial intelligence.

Therefore, this thesis focuses on researching proactive FT strategies to build a FT framework for infrastructure of cloud computing. Accordingly, the FT framework consists of two main components including physical server fault detection of the cloud infrastructure and virtual machine migration. In particular, the proposed anomaly-based fault detector ensures the FT system to work correctly and increases the system's ability to react when a fault occurs. From the results of the fautl detection model, the avoidance of fautl effects will be solved through a virtual machine migration. To improve the responsiveness of the virtual machine migration strategy, this study proposes a virtual machine migration controller capable of reinforcement learning.

2. Main contributions

- Building a proactive FT framework for cloud computing infrastructure based on the MAPE-K loop structure of the autonomous system, including the monitoring component, PM fault analysis, seft-learning VM migration, and resources coordination executing.
- The combination of fuzzy logic and OCSVM (named FOCSVM) is proposed to improve the abnormal detection when outliers appear in the dataset. By using fuzzy logic for calculating penalty factors of OCSVM model, fault detection approach improves flexible operations in real time as well as takes advantage of experts' knowledge. Based on the FOCSVM abnormal detection model, the fault detection and diagnosis approach is proposed including abnormal detection, fault detection, and analysis of suspicious parameters. For fault detection problem, the exponentially weighted moving average (EWMA) chart is then used to identify abrupt changes if there is any fault to occur, named EWMA-FOCSVM. And then, the fault diagnosis problem is abstracted to feature selection problem with the training dataset which are labeled by EWMA-FOCSVM. The analysis of physical server performance parameters related to the

faults is brought to the feature selection problem and solved using the RFE-RF model - which is a combination of the Recursive Feature Elimination (RFE) model and the Recursive Feature Elimination (RFE) model and Random Forest (RF). Suspicious parameters are identified through the feature ranking of the data set.

- The self-learning VM migration component is designed by applying Fuzzy Q-Learning algorithm to enhance the performance of fuzzy inference system. One of the strengths of fuzzy inference systems is their ability to convert human knowledge into intuitive IF-THE rules. VM migration strategies are considered as internal knowledge of the cloud controller which shows capable of learning in the execution environment. To implement the self-learning VM migration controller, a rule set is continually explored during execution time through self-learning rule component which shows ability of self-learning to complete the rule set in run-time without prior knowledge. The migration controller observes the infrastructure state and manipulates the migration plans. The PMs which allocate to cloud-hosted applications are monitored by load balance and abnormal score metrics. The V2PQL algorithm is proposed to migrate VM in order to avoid the influence of deteriorating PMs as well as keep load balance and abnormal score for all the safe PMs. The analysis results from the migration controller go to the self-learning rule component for updating it. Learning mechanism of VM migration rule, named V2PQL-AS, is designed based on a combination of V2PQL algorithm and Ant System algorithm. In general, the problem of VM migration is expressed in the form of one n VMs that need to be migrated into m PM. After migrating VMs, the system ensures at least the level of load balancing between resources in each PM, ensure a minimum of anomalies for each PM, avoid overloading any PM that could lead to degraded performance, and ensure a VM is migrated to only one PM. Therefore, to evaluate the result of the objective function of V2PFQL algorithm, it is necessary to consider at the time of completing the migration of n VMs into m PM. The objective function results of VM migration of V2PFQL algorithm with those of meta-heuristic class including RoundRobin, inverse Ant System (iAS), Ant System (AS), MaxMin Ant System (MMAS), Simulated Annealing (SA), Particle swarm optimization (PSO) algorithms.

Suppervisors **PhD. Candidate**

Assoc. Prof. Tran Cong Hung, Assoc. Prof. Pham Tran Vu **Bui Thanh Khiet**