The Journal of Supercomputing (2019) 75:1–3
https://doi.org/10.1007/s11227-018-2671-4

Performance and security in cloud computing

Weizhong Qiang[1]

© Springer Science+Business Media, LLC, part of Springer Nature 2018

Cloud computing paradigm enables the provision of resources on demand. Cloud computing is dramatically changing the way that organizations manage their resources, owing to its attractive features such as robustness, low cost and ubiquitous nature. Performance and security are the two main concerns of cloud computing. This special issue consists of eight papers addressing the performance and security issues in cloud computing.

The four articles on performance issues are as follows. In the first paper "VMBKS: a shared memory cache system based on booting kernel in cloud", the authors propose VMBKS, which is a cloud shared memory cache system based on booting kernel to solve the "Boot Storm" issue caused by many VMs being boot up simultaneously. They exploit VMs' correlations to organize VM image files, to reduce cache size and mitigate the effect of Boot Storm. They use booting kernel to construct cache and share the booting kernel to correlative VMs. Evaluation results show that VMBKS can speed up VM provisioning time by up to 60% and mitigate the effect of Boot Storm significantly. In the second paper "A lock-aware virtual machine scheduling scheme for synchronization performance", the authors focus on the synchronization problems in multiprocessor virtual machines, such as lock holder preemption (LHP) and lock waiter preemption (LWP). They propose an efficient lock-aware virtual machine scheduling scheme, which detects lock holders and waiters from the virtual machine monitor side, and gives preempted lock holders and waiters multiple, continuous, extra scheduling chances to release locks. The experimental results demonstrate that the scheduling scheme fundamentally eliminates lock holder preemptions and lock waiter preemptions. In the third paper "Resource stealing: a resource multiplexing method for mix workloads in cloud system", the authors focus on the resource multiplexing for the context of heterogeneous workloads. They propose a resource stealing mechanism to improve resource multiplexing of cloud resources, which enables free resource fragments reserved by some workloads to be utilized by others. Experimental results reveal that the proposed algorithms

✉ Weizhong Qiang
wzqiang@hust.edu.cn

[1] School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China

improve resource utilization and workload performance simultaneously. In the fourth paper "Towards a delivery scheme for speedup of data backup in distributed storage systems using erasure codes", the authors focus on a fast backup scheme in distributed systems based on general erasure coding. They propose a scheme that fully takes into account the bandwidths between target storage nodes, rather than only the bandwidths between the source node and target nodes. The benefit is that spare bandwidths between target storage nodes are used to reduce backup time. The experiments show the delay is reduced by 59%, compared with common star-structured scheme. Meanwhile, the throughput is increased significantly in backup process.

The four articles on security issues are as follows. In the fifth paper "Proof of violation for response time auditing in cloud systems", the authors propose to employ the concept of proof of violation (POV) for the response time auditing in the cloud. The POV scheme enables a user or a service provider to produce a precise proof of either the occurrence of the violation of properties or the innocence of the service provider. It is the first scheme that can perform response time auditing according to cryptographic evidences without the need of a delivery agent. Service providers can use the proposed scheme to provide a mutual nonrepudiation guarantee for response time in their service-level agreements. In the sixth paper "A new publicly verifiable data possession on remote storage", the authors propose a new verifiable data possession scheme that supports private and public verifiability simultaneously based on a linearly homomorphic cryptography. In the scheme, the data owner who uses the private verification and anyone else who runs the public verification algorithm simultaneously on the same set of metadata and based on the same setup procedure can securely authenticate the integrity of client's data file stored at cloud server without retrieving the whole original data file. Security analysis of the scheme under several cryptographic assumptions, such as difficulty of Factorization Assumption and Discrete Logarithm Problem (DLP), is also presented. In the seventh paper "A method for achieving provable data integrity in cloud computing", the authors propose a novel method for provable data integrity (PDI) that aims at clients with data stored in untrusted servers. An advantage of this model is the low client cost since a constant amount of metadata is generated. Based on a bilinear group, they propose a simple, efficient audit service for public verification of untrusted outsourced storage. The experimental results show that the proposed method achieves high efficiency. In the eighth paper "A domain-divided configurable security model for cloud computing-based telecommunication services", the authors focus on the issue that traditional device-centric security systems are not effective as resources in the cloud are out of the users control. They propose a domain-divided security model in which different security policies are separately applied for three domains: the data storage domain, the data processing domain and the data transmission domain. Experimental results show that the proposed security model is both practical and lightweight as it can provide differentiated security protection for cloud computing-based telecommunication service with a low overhead.

In closing, we would like to thank all the authors who have submitted their research work to this special issue. We would also like to acknowledge the contribution of many experts in the field who have participated in the review process and provided helpful suggestions to the authors on improving the content and presentation of the papers. We would also like to express our gratitude to the Editor-in-Chief for the support and help in bringing forward this special issue.