Review

for

Performance and Security in Cloud Computing

Cloud computing is a model that enables the provision of resources like data,storage e.t.c. Cloud Computing is completely changing the way of usage of resources,outstanding to its features like robustness,low cost and ubiquitous nature.The two main fields of Cloud Computing are Performance and Security.This special issues consists of eight papers of addressing the performance and security issues in Cloud Computing.

The four articles of performance issues are in the following:

1.VMBKS:"a shared memory cache system based on booting kernel in cloud".

2."A lock-aware virtual machine scheduling scheme for synchronization performance"

3."Resource stealing:a resource multiplexing method for mix workloads in cloud system"

4."Towards a delivery scheme for speedup of data backup in the distributed storage systems using erasure codes"

In this paper in the first issue mainly focused on which is a cloud shared menory cache system based on booting kernel to solve the "Boot Storm" issue caused by many VMs being boot up simultaneouslu .They exploit VMs correlations to organise VM image files,to reduce cache size and mitigate the effect of Boot Strom.this results show that VMBKS can speed up VM provisioning time by up to 60% and mitigate the effect of Boot Storm significantly.

In this paper in the second issue mainly focused on the synchronization problems in multiprocessor virtual machines,such as lock holder preemption(LHP) and lock waiter preemption(LWP).In this efficient lock-aware virtual machine scheduling scheme,which detects lock holders and waiters from the virtual machine monitor side , and gives preemted lock holders and waiters multiple,continuous ,extra sceduling chances to release locks .This experimental results demonstrate that the scheduling scheme fundamentally eliminates lock holder preemtions and lock waiter preemptions.

In this paper in the third issue mainly focused on the resource multiplexing method for the context of heterogeneous work-loads.A resource stealing mechanism to improve resource muliplexing of cloud resources ,which enables free resource fragments reserved by some work-loads to be utilised by others. Experimental results reveal that the proposed algorithms improve resource utilization and workload performance simultaneously.

In this paper in the fourth issue mainly focused on the fast backup scheme in distributed systems based on general erasure coding . A scheme in fully takes into account the bandwidths between target storage

nodes, rather than only the bandwidths between target storage node and target nodes. The experiments show the delay is reduced by 59%,compared with common star-structured scheme.

The four articles on security issues are in the following :

5."Proof of Violation for response time auditing in cloud systems".

6."A new publicly verifiable data possession on remote storage ".

7."A method for achieving provable data integrity in cloud computing ".

8."A domain-divided configurable security model for cloud computing-based telecommunication services".

In this paper in the fifth issue mainly focued 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 occurance of the violation of the violation of properties or the innocence of the service provider. It is the first scheme that can perform resonse time auditing according to cryptographic evidences wihout the need of a delivery agent.

In this paper in the sixth issue a new verifiable data possession scheme that supports private and public verifiability simulatneously 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 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 this paper in the seventh issue a novel method for provable data integrity(PDI) that aims at clints 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 paper in the eighth issue is that traditional device-centric security systems are not affective as resources in the cloud are out of the users control. In this 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 security model is both practicle and lightweight as it can provide differentiated security protection for cloud computing-based telecommunication service with a low overhead.

In closing, in this research thank all the authors who have submitted their research work to this special issue.In this paper 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.In this research also like to express our gratitude to the Editors-in-Chief of the support and help in bringing forward this special issue.