Cloud Computing: Introduction to Virtualization, Energy Saving, and Access Control

John Mui
Athabasca University
1 University Drive
Athabasca, AB T9S 3A3, Canada
April 2017

***Abstract*— In today's rapidly changing landscape of information technologies, one of the fastest growing sectors is the emergence and evolving field of cloud computing. With the goal of resource sharing, usage optimization, and cost reduction, virtualization is a fundamental part of cloud computing, enabling the cloud provider to deliver its service to the customer effectively. The resulting uptake of the cloud has driven cloud data centers, and in particular cloud storage, to become one of the larger consumers of energy. Combinations of techniques such as deduplication and data classification strategy can help to reduce energy consumption. While there is an increase in the usage of cloud services, there are still roadblocks and reluctance due to security concerns. Having proper access control is one way to help improve cloud security.**

Keywords—cloud computing; definition; virtualization; cloud data center; cloud storage; energy optimization; access control; security

I. INTRODUCTION

Due to its ability to provide scalable, cost-effective, and on-demand remote computing services, cloud computing is one of the fastest-growing business solutions within information technology [1]. In [2], the National Institute of Standards and Technology (NIST) defines cloud computing 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." NIST further describes cloud computing with four deployment models - public (available to the general public), private (solely for an organization), community (organizations shared for supporting specific community), and hybrid (combination); three service models of infrastructure (fundamental computing resources), platform (environment for deploying, hosting, and development of application) and software (running application and end functionalities); and five essential characteristics of on-demand self-service (customer's ability to request and manage service dynamically), broad network access (service offered over internet or private network), resource pooling (service draw from pool of computing resources), rapid elasticity (ability to scale up or down) and measured service (usage are measured and billed).

Fundamentally, cloud computing is seen not as a revolution but as an evolution of information systems that combine existing computing technologies [3]. The technological foundation of cloud computing is based on virtualization, distributed technologies such as utility computing, grid computing, and parallel computing, as well as network-related technologies for internet, web service, and enterprise-level networking [4],[5],[6]. The fusion of these various technologies provides a sum that is greater than its individual parts, allowing cloud computing to provide commoditized computing resources to consumers. Companies having one or more applications operating on the cloud went up from 51% in 2011 to 70% in 2016 [7]. However, due to this rapid growth, the consumption of energy by cloud data centers for data storage has resulted in them becoming one of the larger consumers of energy [8]. Moreover, many individuals and corporations have been hesitant to adopt cloud computing technologies due to security concerns [9].

In order to provide a better understanding of this vast field of cloud computing, this paper selectively introduces different areas of cloud computing to the reader. Virtualization, one of the technological foundations of cloud computing, is described in section II. Energy optimization in cloud storage and the advancement to help reduce the consumption of energy within cloud data centers are described in section III. Access control security and the various ways to improve and increase protection in cloud computing are described in section IV. This paper ends with the conclusion in section V.

II. USE OF VIRTUALIZATION IN CLOUD COMPUTING

Cloud computing is built on drivers of the various foundational technologies. One of the key technological foundations is virtualization. This section will introduce the reader to virtualization and provide an overview of the usage of this technology within cloud computing.

Virtualization is a core technology that is fundamental to cloud computing [5], [10]. In simplest terms, virtualizations provide a mechanism that abstracts the physical hardware. This is accomplished with the aid of the hypervisor, a virtual machine monitor that creates, maps, and coordinates access to the resources. Within a virtual machine, a guest operating system and its application are running; whenever they utilize or request system resources, they are accessing and going through a virtual layer. This virtual layer presents an illusion to the consuming program that they are working with the actual resource [5], [10].

The available cloud virtual resources may include processor(s), memory, storage, and network(s) [11-14]. A single physical core may be dedicated to a single virtual processor, or it may be shared between the different virtual processors. In memory virtualization, a logical pool of random access memory is seen by the guest OS, but that memory is coordinated and mapped to physical memory by the hypervisor. For storage virtualization, a seemingly single device to the guest OS may actually be allocated from local physical storage or networked storage such as SAN or NAS. With network virtualization, it will split up the bandwidth and isolate the channel for each of the virtual network interface cards within the virtual machine [11-14].

III. OPTIMIZING ENERGY USAGE IN CLOUD STORAGE SYSTEMS

Cloud data centers are a large consumer of energy, and their storage systems utilize up to 40% of that energy [8]. The majority of that storage energy is consumed by spinning disk drives [15-17]. This section discusses some of the proposals within the last two years dealing with energy efficiency in cloud storage systems and shares the findings with the reader.

A. Determining Classified Storage using Service Level Agreement

In [18], the authors experiment with a low-energy consumption storage method for cloud video surveillance (CVS) data. Customer requirements for video surveillance as a service differ; for example, one may want real-time surveillance from 4 pm to 8 pm, while another may want it all day long. By incorporating domain-specific parameters from CVS, such as access time, quality, and storage, into the service level agreement (SLA), a resource management algorithm derived from the SLA classifications can be used to group and power the associated resources. Their test using SLA-classified storage with 6-time period classifications reduced the number of concurrent running storage nodes by approximately 80%. In general, finer SLA-classified storage results in greater savings.

B. Deduplication Strategy for Storage System in Cloud Environment

In [19], the authors describe a deduplication-based energy-efficient virtual machine storage system (EEVS) for the cloud environment. A way energy consumption can be reduced is by decreasing storage space usage. This can be accomplished by eliminating the redundant data for VM storage. The study looked at reducing both inner-redundancies, duplicate blocks within the VM image, and inter-redundancies, duplicate blocks between different VM images. Their tests showed that booting 10 concurrent VMs using EEVS saved at least a third of the energy compared to traditional systems. In general, a higher deduplication ratio results in more energy savings.

C. Employing Data Classification Strategy in Cloud Storage System

In [20], the authors simulated and adopted a new proposed correlating algorithm based on data classification, named Anticipation-based Green Data Classification (AGDC), to reduce energy consumption in cloud storage systems. AGDC classifies the cloud-based data regions as ‘new’, ‘old’, and ‘seasonal’ from where it is stored in the cloud storage system. It then migrates the data between the regions using the neural network prediction algorithm. Cold data refers to data in the low energy state or cold disk regions that are not accessed frequently. Hot data refers to data in the high-energy state or hot disk regions where it is accessed frequently. The temperature of the data is predicted by the neural network algorithm. In simulation experiments, using the AGDC resulted in a reduction in energy usage by 16%.

D. A Hybrid Approach to Cloud Storage Energy Saving

It is this author’s recommendation for a hybrid approach, which uses a combination of data classification and deduplication with service level agreement to reduce cloud storage energy usage. First, utilize the SLA to our advantage by segregating consumers with similar operating hours together. When in non-operation hours, these customers’ hard drives can be completely shut down. Next, deduplication should be applied to safely remove identical repeated data without negatively impacting customer data redundancy and availability. Lastly, the data will be grouped based on usage pattern classification. Those with data that are accessed infrequently can be placed on slower spin low-energy disk drives.

IV. STRATEGIES AND TECHNIQUES IN ACCESS CONTROL TO IMPROVE CLOUD SECURITY

The adoption of cloud computing has been hampered by privacy, compliance, regulatory, and most significantly, security issues [1]. This section explores a general aspect of cloud security via access control, describing access control strategies and techniques that can be employed to improve cloud computing security.

Data access control and management relates to the user’s ability to retrieve and access data stored within the cloud environment [21], [22]. Authentication, a process to determine user identities, and authorization, a process to determine permission rights, are some of the key factors for maintaining access security [23]. In order to achieve proper authorization, the least privilege model should be followed. In the least privilege model, both the user and cloud service administrator are given sufficient rights to perform their duties (where the rights are regularly reviewed); however, they are not given over-sufficient or under-sufficient permissions [23]. In terms of authentication, a method to achieve extra strong authentication (for example, in military cloud installation with custom equipment) is to use robust multi-factor authentication. This author put forward one such advanced multi-factor authentication, which combines something the user knows (password plus shared secret challenge question known to the user), something the user owns (smart card plus passcode key token), something the user is via static biometric (fingerprint plus retina scan) and dynamic biometric (handwriting plus voice, for writing comparison and vocal recognition of a generated sentence).

An Access Control List (ACL) mechanism, such as those based on the Amazon S3 specification, can provide a user the ability to assign policies to groups, specific users, or data container buckets [24]. In more complex enterprise cloud environments, integration with complementary approaches such as Role-based Access Control (RBAC) may be appropriate. Research advancement into fine-grained access control can provide a more in-depth method that intermixs access control into data protection. One such technique is to integrate actual authorization policies into the data itself. The result is only those who are authorized can decrypt it [24]. Another proposed cloud access control technique [25] involves minimal communication overhead with methods that limit the information a cloud provider can learn from the partial view of access rules and patterns. This methodology works on the client's end to process read and write access control. Additional access control techniques, such as xAccess, described in [26], incorporate a mechanism to empower the individual cloud user to assign their own access policy for the sharing of user-created content. This is especially useful in cloud social media applications, where the sharing of profiles, videos, and blogs is popular.

Another sometimes overlooked but important aspect of access control relates to physical access [9]. Whenever someone with malicious intent is physically present within the premise of the cloud data center, overall security can be significantly affected. This author postulates in a physical break-in of a cloud provider; there will be a number of negative possibilities: thefts can steal the servers that multiple tenants use, cut the power cord to the equipment, and physically destroy the hardware, all affecting availability and beyond. Some possible deterrents that this author proposes are patrolling security guards, electronic and key-locked doors, alarm systems, and building access policies. A subtler on-location attack can be performed by malicious insiders, where the most successful ones are never discovered. In order to lessen the possibility of such an attack, proper enforcement procedures should be established for monitoring, detection, and prevention, with the use of security cameras, activity log reviews, continual employee background, and financial checks [27].

V. CONCLUSION

Many of the advantages associated with cloud computing are in part due to the flexibility provided by virtualization [28], [29]. Since resources are virtualized, they can be scaled up or down dynamically by reallocating or de-allocating from the pooled resources. Improvement in fault tolerance and resiliency can be achieved by migrating virtual resources off the failing devices and moving them onto a different host. Moreover, the ability to run multiple virtual machines on one set of hardware can increase usage efficiency, leading to cost and energy reduction.

The increased uptake of cloud computing has instigated energy usage concerns. Reducing storage space requirement via deduplication can lead to using fewer disk drives; therefore, fewer drives consume energy. Classifying infrequently accessed data by grouping them onto a storage drive that spins for less time can increase energy efficiency. Using SLA to determine whenever drives are not being accessed so those unused drives can be in off/low power mode can also lead to energy saving. The various methods are not without drawbacks that can impact performance, availability, and consistency [18-20]. However, each method and combination of them are a prospective solution for energy-efficient data storage in cloud environments, making them a potentially viable option available for data center operators to achieve energy saving.

There are still many serious barriers to the adoption of cloud computing, the most critical one being security issues [30]. One potential solution is to put proper access control into place. Having good access control can have a positive contribution to securities' confidentiality, integrity, and availability. With the proper use of access control, confidentiality can be achieved by preventing unauthorized users from accessing sensitive information. Integrity can be maintained as the removal and modification of data is controlled and granted only to the proper users. Furthermore, availability can improve since all non-authorized users cannot access the data; this frees up processing for only those who can access the information in a reliable and timely manner.

REFERENCES

[1] S. Singh, Y. Jeong, and J. H. Park, "A survey on cloud computing security: issues, threats, and solutions." Journal of Network and Computer Applications, 75(2016), 200-222.

[2] P. Mell, and T. Grance, "The NIST definition of cloud computing." National Institute of Standards and Technology, 53(6), 50. 2011

[3] N. Phaphoom, X. Wang, and P.Abrahamsson, "Foundations and technological landscape of cloud computing." ISRN Software Engineering, 2013.

[4] T. Erl, Z. Mahmood, and R. Puttini, "Cloud Computing: Concepts, Technology & Architecture", 2016. Retrieved from: http://www.whatiscloud.com/origins_and_influences/technology_innovations

[5] M. Carroll, A. Van Der Merwe, and P. Kotze, "Secure cloud computing: Benefits, risks and controls." In Information Security South Africa (ISSA), 2011, pp. 1-9. IEEE, 2011.

[6] P. Raj, "The Network Infrastructures for Big Data Analytics," in Handbook of Research on Cloud Infrastructures for Big Data Analytics, P. Raj and G. Deka, Eds. Hershey, PA: IGI Global, 2014, pp. 157-185.

[7] IDG Enterprise, "Cloud Adoption Goes Mainstream, Yet Security Remains Top of Mind", 2016 IDG Enterprise Cloud Computing Survey. Retrieved from: http://www.idgenterprise.com/news/press-release/cloud-adoption-goes-mainstream-yet-security-remains-top-mind/

[8] C. Negru, F. Pop, V. Cristea, N. Bessisy, and J. Li, "Energy Efficient Cloud Storage Service: Key Issues and Challenges". 2013 Fourth International Conference On Emerging Intelligent Data & Web Technologies, 763, 2013.

[9] A. Singh, and K. Chatterjee, "Review: Cloud security issues and challenges: A survey." Journal Of Network And Computer Applications, 7988-115, 2017.

[10] N. Phaphoom, W. Xiaofeng, and A. Pekka, "Foundations and technological landscape of cloud computing." ISRN Software Engineering 2013.

[11] R. Kumar, and C. Shilpi, "An importance of using virtualization technology in cloud computing." Global Journal of Computers & Technology Vol 1, no. 2, 2015.

[12] A. Younge, R. Henschel, J. Brown, G. Von Laszewski, J. Qiu, and G. Fox, "Analysis of virtualization technologies for high performance computing environments." In Cloud Computing (CLOUD), 2011 IEEE International Conference on, pp. 9-16. IEEE, 2011.

[13] K. Khajehei, "Role of virtualization in cloud computing." International Journal of Advance Research in Computer Science and Management Studies 2, no. 4, 2014.

[14] M. Durairaj , P. Kannan , " A Study on Virtualization Techniques and Challenges in Cloud Computing ." International Journal of Scientific & Technology Research, vol. 3, issue 11, pp. 147 – 151, November 2014.

[15] D. Vellante, "Storage energy consumption," 2010. [Online]. Available: http://wikibon.org/wiki/v/Storage_energy_consumption. Accessed: Feb. 21,2017.

[16] ProcessFlows, "Spinning HD drives use up 80% of server power costs," 2013.[Online].Available: https://processflows.co.uk/uncategorized/spinning-around/. Accessed: Feb. 21, 2017.

[17] C. Karakoyunlu and J.A. Chandy, "Exploiting user metadata for energy-aware node allocation in a cloud storage system". Journal Of Computer And System Sciences, 82282-309. 2015

[18] Y. Xiong, C. Lu, M. Wu, K. Jiang, and D. Wang "A Low Energy Consumption Storage Method for Cloud Video Surveillance Data Based on SLA Classification". Mobile Information Systems, 2016.

[19] H. Li, M. Dong, X. Liao, and H. Jin, "Deduplication-Based Energy Efficient Storage System in Cloud Environment". Computer Journal, 58(6), 1373-1383. 2015

[20] X. You, C. Dong, L. Zhou, J. Huang, and C. Jiang, "Anticipation-based Green Data Classification Strategy in Cloud Storage System". Applied Mathematics & Information Sciences, 9, 4 (2015), 2151. 2015

[21] B. Jeevitha, J. Thriveni, and K. Venugopal, "Data Storage Security and Privacy in Cloud Computing: A Comprehensive Survey". International Journal of Computer Applications, 156(12). 2016.

[22] C. Langaliya, and R. Aluvalu, "Enhancing Cloud Security through Access Control Models: A Survey". International Journal of Computer Applications, 112(7). 2015

[23] P. Ashok, "Protecting Healthcare Database by Access Control Method on Cloud Computing Technique-A Survey". International Journal of Advanced Research in Computer Science, 6(1). 2015

[24] R. Roman, M. R. Felipe, P. E. Gene, and J. Zhou, "Complying with Security Requirements in Cloud Storage Systems". JCP, 11(3), 201-206. 2016

[25] S. Beulah, and F. Dhanaseelan, "Survey on security issues and existing solutions in cloud storage". Indian Journal of Science and Technology, 9(13). 2016

[26] B. Balamurugan, N. Shivitha, V. Monisha, and V. Saranya, "Survey of access control models for cloud based real-time applications". In Innovation Information in Computing Technologies (ICIICT), 2015 International Conference on (pp. 1-6). IEEE. 2015

[27] A. Duncan, S. Creese, and M. Goldsmith, "An overview of insider attacks in cloud computing." Concurrency & Computation: Practice & Experience, 27(12), 2964-2981. 2015

[28] K. Divya, and S. Jeyalatha, "Key technologies in cloud computing." In Cloud Computing Technologies, Applications and Management (ICCCTAM), 2012 International Conference on, pp. 196-199. IEEE, 2012.

[29] L. Malhotra, D. Agarwal, and A. Jaiswal, "Virtualization in cloud computing." J Inform Tech Softw Eng 4, no. 2 : 136, 2014.

[30] A.K. Dhingra, and D. Rai, "Evaluating risks in cloud computing: Security perspective," in 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 533-536. 2016