Consistency and Privacy based Replication System in Cloud Sharing Framework

Sathees Kumar J*, Romeo J*
*UG Scholar,
Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan College of Engineering,
Perambalur, TamilNadu, India.

Sathish Kumar P*
+ Assistant Professor,
Department of Computer Science and Engineering,
Dhanalakshmi Srinivasan College of Engineering,
Perambalur, TamilNadu, India.

Abstract- Outsourcing data can be lead many security problems in cloud storage. So implement privacy preserving data storage using DROPS based access control mechanism. Prevent data storage from unauthorized access. With the increase in cloud service providers, and the increasing number of compute services offered, a migration of information systems to the cloud demands selecting the best mix of compute services and VM (Virtual Machine) images from an abundance of possibilities. That is, an end user could be cheated into accepting a wrong or maliciously transformed output. In this paper, we first formalize a security model of ABE with verifiable outsourced decryption by introducing verification key in the output of the encryption algorithm. Currently, there is no detailed study available centering the DCN robustness. Therefore, we believe that this study will lay a firm foundation for the future DCN robustness research. In particular, we present an evolutionary migration process for web application clusters distributed over multiple locations, and clearly identify the most important criteria relevant to the selection problem. Moreover, we present a multi criteria-based selection algorithm based on Analytic Hierarchy Process (AHP). Because the solution space grows exponentially, we developed a Genetic Algorithm (GA)-based approach to cope with computational complexities in a growing cloud market.

Keywords - Drops, T-Coloring Algorithm—cloud migration data sharing, decryption outsourcing

I. INTRODUCTION

Data encryption using symmetric or public key cryptography is not amenable to scalable access control. A promising approach to address this issue is attribute-based encryption (ABE), first proposed by Sahai and Waters [1]. ABE schemes can be divided into two categories: Cipher text Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE) [2], depending on the access policy is embedded into the cipher text or the user's private key However, a drawback of the standard ABE schemes is their relatively large cipher text size and high decryption cost, and this problem is especially acute for resource limited devices such as mobile devices.

Specifically, in an ABE scheme, the size of the cipher text and the cost of decryption grow with the complexity of the access structures/policies. Moreover, current constructions of ABE schemes, see [2]–[5], rely on pairing-based groups and require many pairing operations (which are usually more expensive than exponentiations) in decryption Cloud computing is a disruptive technology and an adoption brings along risks and obstacles. Risks can turn into effective problems or disadvantages for organizations that may decide to move web applications to the cloud. Such a decision depends on many factors, from risks and costs to security issues, service level and QoS expectations. A migration from an organization-owned data center to a cloud infrastructure service implies more than few trivial steps. Steps of a migration to PaaS offerings, such as Google App Engine, would differ in several regards.

The significance of the interconnection networks is obvious from the aforementioned discussion, providing adequate evidences for the robustness requirement of the network. It can be inferred from the discussion that the network robustness holds a key role to ensure desired level of performance and QoS in cloud computing. In the said perspective, measuring the robustness of the DCN is crucial to identify the behavior and level of performance that a network can attain under perturbations and failure-prone circumstances. Therefore, DCN's robustness is a vital measure for proven performance and fault tolerance in cloud

The Three Tier DCN is the most commonly used DCN architecture [16]. The Three Tier DCN is a switch-centric architecture and the network devices are organized in three layers namely: 1) access, 2) aggregate, and 3) core network layer. The access layer switch connects various computational servers within a rack. Multiple access layer switches are connected to the aggregate layer switches. The core layer switches are used to connect all of the aggregate layer switches.

II. RELATED WORK

Cryptographic protection on outsourced data storage has been considered (see survey in [8]). For example, Wang et al. [23] propose secure outsourced data access mechanisms that support changes in user access rights and outsourced data. A teniese et al. [4] and Wang et al. [22] propose an auditing system that verifies the integrity of outsourced data. However, all the above systems require new protocol support on the cloud infrastructure, and such additional functionalities may make deployment more challenging. Security solutions that are compatible with existing public cloud storage services have been proposed. Yun et al. [24] propose a cryptographic file system that provides privacy and integrity guarantees for outsourced data using a universal hash based MAC tree. They prototype a system that can interact with an untrusted storage server via a modified file system. Jungle Disk [7] and Cumulus [21] are proposed to protect the privacy of outsourced data, and their implementation use Amazon S3 [2] as the storage backend. Specifically, Cumulus

focuses on making effective use of storage space while providing essential encryption on outsourced data.

The above systems mainly put the protocol functionalities on the client side, and the cloud storage providers merely provide the storage space. The concept of attributed-based encryption (ABE) is first introduced in [17], in which attributes are associated with encrypted data. Goyal et al. [6] extend the idea to key-policy ABE, in which attributes are associated with private keys, and encrypted data can be decrypted only when a threshold of attributes are satisfied. Pirretti et al. [16] implement ABE and conduct empirical studies. Nair et al. [12] consider a similar idea of ABE, and they seek to enforce a fine grained access control of files based on identity-based public key cryptography. Perlman et al. [15] also address the Boolean combinations of policies, but they focus on digital rights management rather than file assured deletion and their operations of cryptographic keys are different from our work because of the different frameworks. As argued in Section 2.2, ABE and our work have different design objectives and hence different key management mechanisms.

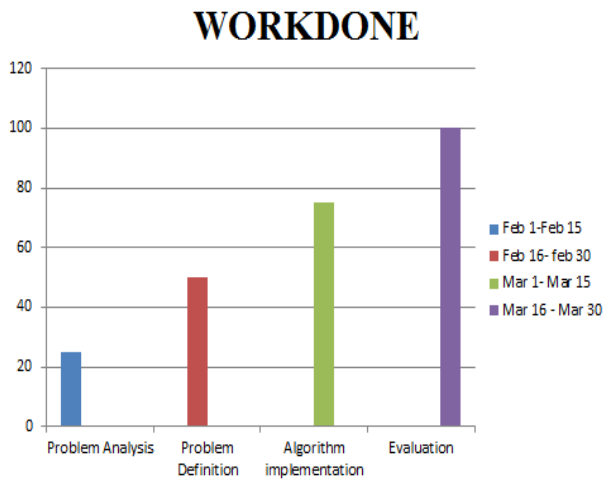


Fig. 1 Cloud computing datacenter

2.1 Relevant Peer Research

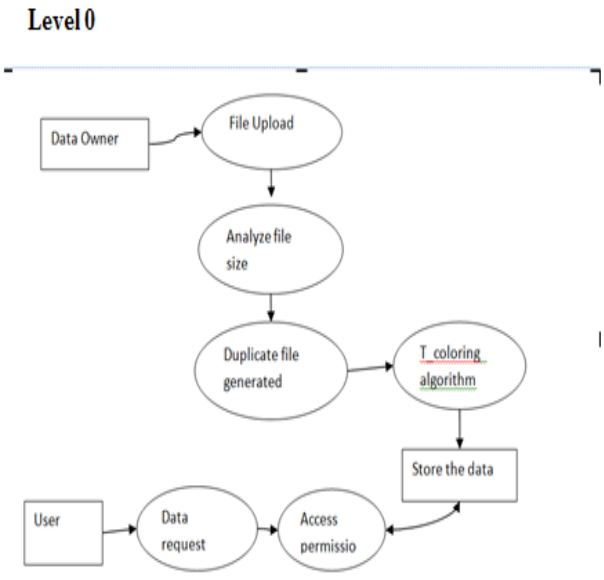
Wide-Area Network (WAN) Datacenters2, 3,…,N
Central DB
Datacenter DB
Rack DB
Aggregation Network
Access Network
Core Network
Central DB Access Data center DB Access Rack DB Access Rack
Time (t)
a (t)
a0

Fig. 2 Data access distribution typically in the range [30,31], which depends on the type of the content [27].

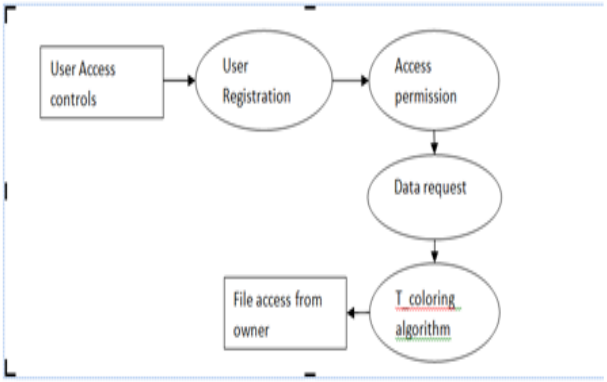
Figure 2 presents a plot of Eq. (1). The access rate can be obtained as the first derivative from Eq. (1). ra (t) = da dt. (2) Whenever cloud applications access data items, they can modify them with some probability updating the database. Therefore, the update rate can be expressed as a fraction of the access rate. Ru (t) = ρ ·ra (t), (3) where [0, 1] control relation between the access rater a(t) and the update rate. For ρ = 1, cloud applications modify
Every data item they access, while for ρ =0 these modifications is never performed. Figure 3 presents the timeline of a workload execution in data center. It begins with the user request arrival at the data center gateway. After being scheduled it is forwarded through the data center network to the selected computing resource for execution. At the server, the workload can request data item if it is needed for its execution. For this, it queries a data base and waits for the database reply to arrive. The database querying delay corresponds to the round-trip time and depends on the database location. As soon as the database reply is received, the workload execution is started. At the end of the execution, some workloads will send a modified data item back to the database for the update. As a result, the total delay associated with the workload execution in datacenters can be computed as follows: ddc =dreq+2·ddb+dexec+dupdate, (4) where dreq is a time required for the work load description to arrive at the computing server, ddb is a one-way communication delay between the server and the database, dexec is a workload execution time which is defined by the size of the computing work of the workload and computing speed of the server, and d update is the time required to update database.

2.2 Cloud computing system architecture

Large-scale cloud computing systems are composed of geographically distributed across the globe data centers (see Fig. 1). The most widely used data center topology is the three tier fat tree [31], which consists of three layers of net



Level 2:



III. PROBLEM ANALYSIS

The scope of this paper is the DROPS methodology; we divide a file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment a particular data file that ensures that even in case of successful attack, no meaningful information is revealed to the attacker. There is no security and improved performance in replication problem. Difficult to select the data nodes based on distances. There is no security and improved performance in replication. aim of this paper is Division and Replication of Data in the Cloud for Optimal Performance and Security (DROPS) that collectively approaches the security and performance issues.

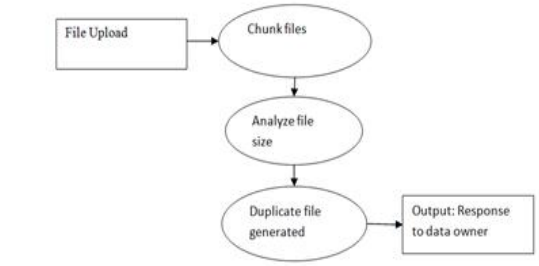
3.1 Comparative techniques

We compared the results of the DROPS methodology with fine-grained replication strategies, namely: (a) DRPA-star, (b) WA-star, (c) A -star, (d) SA1, (e) SA2, (f) SA3, (g) Local Min-Min, (h) Global MinMin, (i) Greedy algorithm, and (j) Genetic Replication Algorithm (GRA). The DRPA-star is a data replication algorithm based on the A-star best-first search algorithm. The DRPA-star starts from the null solution that is called a root node. The communication cost at each node n is computed as: cost(n)=g(n)+h(n), where g(n) is the path cost for reaching n and h(n) is called the heuristic cost and is the estimate of cost from n to the goal node.

The DRPA-star searches all of the solutions of allocating a fragment to a node. The solution that minimizes the cost within the constraints is explored while others are discarded. The selected solution is inserted into a list called. There is no security and improved performance in replication problem. Difficult to select the data nodes based on distances. Cloud security follows traditional cryptography approach includes encryption and decryption. Cryptography includes symmetric and asymmetric approaches User based access control mechanism can be used at the time of data access by users.

3.2 Analysis

Level 1:



We compared the performance of the DROPS methodology with the algorithms discussed in Section 5.1. The behavior of the algorithms was studied by: (a) increasing the number of nodes in the system, (b) increasing the number of objects keeping number of nodes constant, (c) changing the nodes storage capacity, and (d) varying the read/write ratio. The aforesaid parameters are significant as they affect the problem size and the performance of algorithms [13].

5.3.1 Impact of increase in number of cloud nodes we studied the performance of the placement techniques and the DROPS methodology by increasing the number of nodes. The performance was studied for the three discussed cloud architectures. The numbers of nodes selected for the simulations were 100, 500, 1,024, 2,400, and 30,000. The number of nodes in the Dcell architecture increases exponentially [2]. For Dcell architecture, with two nodes in the Dcell0, the architecture consists of 2,400 nodes.

However, increasing a single node in the Dcell0, the total nodes increases to 30, 000 [2]. The number of file fragments this article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TCC.2015.2400460, IEEE Transactions on Cloud Computing In this module, we maintain the website to gather the blood donor's details such as registration details, donor's details and blood details.

3.2 CLOUDGENIUS FOR WEB APPLICATIONS

To additionally support migrations of web applications with a compute cluster architecture (referred to as web application clusters) to cloud infrastructures, we propose an extension of the Cloud Genius framework. One feature of the extended framework is the evolutionary cloud migration process model. The process model integrates existing migration approaches and methods to support multi-criteria-based decisions to select cloud VM images and compute services for multiple components.

In the following subsections, we present the process model for multi component migrations of web application clusters and give details on the formal model. Moreover, we point out required user input and flexibilities, and present methods to select VM images and services from the abundance of offerings. Finally, we give insights into the evaluation of clusters considering network costs and constraints, and look into computational complexities.

VI. CONCLUSION

In this paper, we presented the extended Cloud Genius framework, which provides a hybrid approach that combines multi-criteria decision making technique with evolutionary optimization technique for: (i) helping application engineers with the selection of the best service mix at IaaS layer and (ii) enabling migration of web application clusters distributed across clouds. We proposed the DROPS methodology, a cloud storage security scheme that collectively deals with the security and performance in terms of retrieval time. The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by means of T-coloring. The fragmentation and dispersal ensured that no significant information was obtainable by an adversary in case of a successful attack. No node in the cloud, store more than a single fragment of the same file. The performance of the DROPS methodology was compared with full-scale replication techniques. The results of the simulations revealed that the simultaneous focus on the security and performance resulted in increased security level of data accompanied by a slight performance drop.

REFERENCES

[1] A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Advances in Cryptology (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp. 457–473. [2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[2] “Web Application Hosting in the AWS Cloud Best Practices,” http://media.amazonwebservices.com/AWS Web Hosting Best Practices.pdf, accessed 2013-07-19., Amazon Web Services. [2] M. Armbrust, A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al., “Above the Clouds: A Berkeley View of Cloud Computing,” EECS Department, University of California, Berkeley, Tech.Rep.UCB/EECS2009-28, 2009.

[3] Buyya, R., Yeo, C.S., Venugopal, S.: Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities. In: IEEE International Conference on High Performance Computing and Communications (HPCC), pp. 5–13. Dalian, China, (2008).

[4] K. Bilal, S.U.R. Malik, O. Khalid, A. Hameed, E. Alvarez, V. Wijaysekara, R. Irfan, S. Shrestha, D. Dwivedy, M. Ali, U.S. Khan, A. Abbas, N. Jalil, and S.U. Khan, “A Taxonomy and Survey on Green Data Center Networks,” Future Generation Computer Systems, 2013.

[5] Amazon. SmugMug Case Study: Amazon Web Services. http://aws.amazon.com/ solutions/case-studies/smugmug/, 2006. 2. Amazon Simple Storage Service **(Amazon S3).** http://aws.amazon.com/s3/. 3. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[6] Vaquero L.M., Rodero-Merino L, Caceres J., Lindner M. A break in the clouds: towards a cloud definition. In: ACM SIGCOMM, editor. Computer communication review 2009. New York: ACM Press; 2009.

[7] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing,2009.

[8] Peter Mell, Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST. 2011.

[9] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing(v2.1). December, 2009.