

Experimental Analysis on Protocol in Cloud Computing using Shared Authority based Privacy-Preserving Authentication

Parul¹, Mr. Sunil Maggu²

¹Department of Computer Science & Engineering Vaish College of Engineering, Rohtak
Assistant Professor Department of Computer Science & Engineering Vaish College of Engineering, Rohtak

ABSTRACT

Trust and security have prevented businesses from fully accepting cloud platforms. To protect clouds, providers must first secure virtualized datacenter resources, uphold user privacy, and preserve data integrity. The authors suggest using a trust-overlay network over multiple data centers to implement a reputation system for establishing trust between service providers and data owners. In this paper, we investigate the problem of data security in cloud data storage, which is essentially a distributed storage system. To achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users, we propose an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. We rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability.

INTRODUCTION

Two significant computer advances – cloud technology and powerful cloud devices – are revolutionizing how users work and the degree of control they experience over their data. Cloud computing is catalyzing a migration from in-house infrastructure and applications to remote public infrastructure and Web services; as a result, personal desktop applications are yielding to Web services – such as Google Docs and Photoshop Express – and IT-managed enterprise applications and datacenters to cloud-based solutions – such as Amazon AWS. Further, robust and usable small-form portable devices are encouraging users to adopt increasingly cloud computing habits. For example, travelers can carry gigabytes of data on their laptops and USB sticks, access calendars and emails on phones, and read documents with e-readers.

While cloud and cloud computing enable pervasive data access and large-scale sharing, they also threaten users' sense of control over their data's security, privacy, and management. For example, when sending an email over Hotmail, posting a photo to Facebook, or uploading a document on Google Docs, users cede all data control to the Web service. The service can decide to retain the data for months after the user requests its deletion, to share it with others for monetary or legal reasons, or to replicate it on servers outside the user's jurisdiction. However detrimental, such practices are commonplace today [38, 140, 184, 219]. Similarly, losing a cloud device means users cannot securely erase their data, prevent access to it by thieves, or identify potentially compromised data.

This dissertation examines the data security, privacy, and management challenges created by clouds and new cloud technologies, and propose novel techniques to re-empower users with control over their data stored on them. By analyzing new cloud and cloud technologies, we identify three root causes for the lost data control: (1) the untrustworthy and possibly hostile computing environments in public clouds and on stolen cloud devices, (2) the lack of customizability that characterizes these environments, and (3) data dissemination across many clouds and devices. These properties challenge users' ability to perform many tasks, such as obtaining an audit log of all accesses to data, securely erasing sensitive data, customizing various data-management properties (such as where a service should replicate data), and organizing personal data meaningfully when it is scattered across many services and devices.

LITERATURE REVIEW

Conventional wisdom suggests that standard encryption systems, such as Bit Locker [130], PGP Whole Disk Encryption [153], and True Crypt [70], can protect confidential information. However, encryption alone is sometimes insufficient to meet users' needs. Two reasons are relevant for this discussion.

Cloud computing has been cited as ‘the fifth utility’ (along with water, electricity, gas, and telephone) whereby computing services are readily available on demand, like other utility services available in today’s society [Buyya, Yeo, Venugopal, Broberg, and Brandic, 2009]. This vision is not essentially new. Dating back to 1961, John McCarthy, retired Stanford professor and Turing Award winner, in his speech at MIT’s Centennial, predicted that in the future computing would become a ‘public utility’ [Wheeler and Waggener, 2009]. In 1969, Leonard Kleinrock, one of the chief scientists of the original Advanced Research Projects Agency Network (ARPANET) project which seeded the Internet, said: ‘As of now, computer networks are still in their infancy, but as they grow up and become sophisticated, we will probably see the spread of “computer utilities” which, like present electric and telephone utilities, will serve individual homes and offices across the country’ [Kleinrock, 2005, p. 4]. It could be argued that cloud computing has begun to fulfil this vision of computing on demand.

Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. storage, processing, bandwidth, and active user accounts) [Mell and Grance, 2009].

DISCUSSION

Cloud Computing architecture, just like any other application or software, is considered into two main sections: Front End and Back End. Front end is a client or any application which is using cloud services. Back end is the network of client machines with servers having computer program and data storage system. Cloud has centralized server administration to administrate the systems client, demands etc. Once user scenarios are developed and the test is designed, and executed. Once the test completed the cloud service provider deliver results and analytics back to corporate IT professionals through real-time dashboards for a complete analysis of how their applications and the internet will perform during peak volumes

The process of analyzing software applications and supporting infrastructure to determine acceptable performance ,capacity and transaction handling capabilities of real world data with usage conditions and executing them against the application and supporting infrastructure under test. The basic approaches to performing load testing on a Web application are: Identify the performance-serious states. Identify the workload status for distributing the entire load among the key scenarios. Identify the metrics to verify them against your performance objectives. Design tests to simulate the load. Use available tools to implement the load according to the designed tests, and capture the metrics for proper load analysis. Identify and analyze the metric data captured during the tests; make a record for proper load spreading. By such an iterative testing process, we achieve our performance objectives. The basic need of load testing is used to govern the Web application’s behavior under both usual and foreseen peak load conditions. Performance testing eliminates the constraints of traditional testing solutions like hardware availability, software licensing and installation, version control, test creation, system monitoring, and the cost of hiring and training staff.

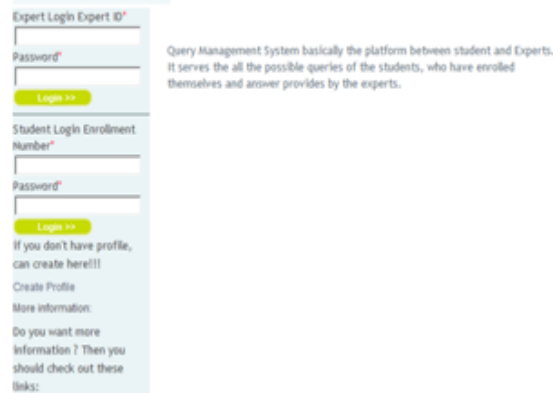
To verify application's support for various browser types and performance in each type can be accomplished with ease. Many tools enable automated website from the cloud.

RESULT

The process of analyzing software applications and supporting infrastructure to determine acceptable performance ,capacity and transaction handling capabilities of real world data with usage conditions and executing them against the application and supporting infrastructure under test. The basic approaches to performing load testing on a Web application are: Identify the performance-serious states.

Identify the workload status for distributing the entire load among the key scenarios.

Identify the metrics to verify them against your performance objectives. Design tests to simulate the load. Use available tools to implement the load according to the designed tests, and capture the metrics for proper load analysis. Identify and analyze the metric data captured during the tests; make a record for proper load spreading. By such an iterative testing process, we achieve our performance objectives. Here the user or student can store the data on cloud, ask the queries and the answers are provided by the expert.



Expert Login Expert ID*
Password*
[Login >>](#)

Student Login Enrollment Number*
Password*
[Login >>](#)

If you don't have profile, can create here!!!
[Create Profile](#)
[More information](#)

Do you want more information? Then you should check out these links:

Query Management System basically the platform between student and Experts. It serves the all the possible queries of the students, who have enrolled themselves and answer provides by the experts.

Fig. 1 Home page



Hi... parul kadlan.!!!

- ▶ [UPDATE PROFILE](#)
- ▶ [CHANGE PASSWORD](#)
- ▶ [SUBMIT QUERY](#)
- ▶ [VIEW QUERY](#)
- ▶ [LOGOUT](#)

[Submit Query](#)

Name: parul kadlan Enrollment Number: par917
Email ID: p1@gmail.com Course: m.tech
Contact Number: 9034355706

Subject*:
Topic*:
Query*:

[Submit Query](#)

Fig. 2 Submit query page



Hi... parul kadlan.!!!

- ▶ [UPDATE PROFILE](#)
- ▶ [CHANGE PASSWORD](#)
- ▶ [SUBMIT QUERY](#)
- ▶ [VIEW QUERY](#)
- ▶ [LOGOUT](#)

[View Query](#)

Submitted Query: what is the full form of sql?
Query Topic: sql
Query Subject: dbms
Query Submission Time: 19/06/2016 06:06
Answer of Query:

Fig. 3 View Query Page

CONCLUSION

We identify a new privacy challenge during data accessing in the cloud computing to achieve privacy-preserving access authority sharing. Authentication is established to guarantee data confidentiality and data integrity. Data anonymity is achieved since the wrapped values are exchanged during transmission. User privacy is enhanced by anonymous access requests to privately inform the cloud server about the users' access desires. Forward security is realized by the session identifiers to prevent the session correlation. It indicates that the proposed scheme is possibly applied for enhanced privacy preservation in cloud applications.

REFERENCES

- [1]. Linghao Zhang, Tao Xie, Nikolai Tillmann, "Environment Modeling for Automated Testing of cloud Applications.
- [2]. http://en.wikipedia.org/wiki/cloud_testing
- [3]. A Vanitha Katherine, K Alagarsamy, "Software Testing in Cloud Platform: A Survey", IJCA, May2012
- [4]. Srinivas Rao V, Nageswara Rao N K, E Kusum Kumari "Cloud Computing : An Overview", JATIT (www.jatit.org)
- [5]. erry Gao, Xiaoying Bai and Wei -Tek Tsai, "Cloud Testing - Issues, Challenges, Needs and Practice", SEIJ, September2011. [6] W.K. Chan, Lijun Mei and Zhenyu Zhang, "Modeling and Testing of Cloud Applications", IEEE APSCC 2009.
- [6]. Michel, Armbrust, "A view of cloud Computing."
- [7]. White papers by cognizant, "Taking Testing to the cloud".
- [8]. White Papers by Deloitte, "Cloud Computing -a collection of Working Papers".
- [9]. White Paper on "Cloud Computing Use Cases Discussion Group".
- [10]. Michael Armbrust Armando Fox, Rean Griffith, "Above the Clouds: A Berkeley View of Cloud Computing".
- [11]. White Paper by Think Grid, "Introduction to Cloud Computing".