International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/IJSRCSEIT

Increased Performance In Resource Allocation System

Janakiraman M[1], Bala Murali Krishnan J[1], Nickelson S[1], Nihas Ahamed I[1], Ms. K.Veena[2]

[1]UG Scholar, [2]Asststant Professor,

Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Coimbatore, Tamil Nadu, India

ABSTRACT

Article Info
Volume 7, Issue 2
Page Number: 425-431

Publication Issue :
March-April-2021

Article History
Accepted : 18 April 2021
Published : 24 April 2021

Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance, so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, propose a secure cloud storage system supporting privacy-preserving public auditing. Further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Keywords : Cloud Computing. Cloud Storage, Integrity, Privacy-preserving, TPA.

I. INTRODUCTION

Cloud computing is the delivery of different services through the Internet. These resources include tools and applications like data storage, servers, databases, networking, and software. Rather than keeping files on a proprietary hard drive or local storage device, cloud-based storage makes it possible to save them to a remote database. As long as an electronic device has access to the web, it has access to the data and the software programs to run it. Cloud computing is a popular option for people and businesses for a number of reasons including cost savings, increased productivity, speed and efficiency, performance, and security. Cloud computing is named as such because the information being accessed is found remotely in the cloud or a virtual space. Companies that provide cloud services enable users to store files and applications on remote servers and then access all the data via the Internet. This means the user is not required to be in a specific place to gain access to it, allowing the user to work remotely. Cloud computing takes all the heavy lifting involved in crunching and processing data away from the device you carry around or sit and work at.

Cloud computing is the provision of dynamically scalable and often virtualized resources as a services over the internet Users need not have knowledge of, expertise in, or control over the technology infrastructure in the "cloud" that supports them. Cloud computing represents a major change in how we store information and run applications. Instead of hosting apps and data on an individual desktop computer, everything is hosted in the "cloud"—an assemblage of computers and servers accessed via the Internet.

Cloud computing exhibits the following key characteristics:

- Agility improves with users' ability to re-provision technological infrastructure resources.
- Multi tenancy enables sharing of resources and costs across a large pool of users thus allowing for:
- Utilization and efficiency improvements for systems that are often only 10–20% utilized.
- Reliability is improved if multiple redundant sites are used, which makes well-designed cloud computing suitable for business continuity and disaster recovery.
- Performance is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.
- Security could improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford. However, the complexity of security is greatly increased when data is distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. In addition, user access to security audit logs may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.
- Maintenance of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.

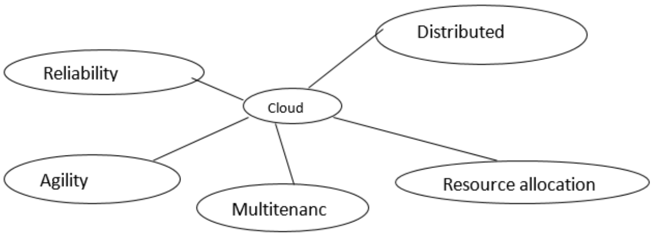


Fig 1 Cloud Computing

II. Related Work

A) Performance Anomaly Detection and Bottleneck Identification.

In order to meet stringent performance requirements, system administrators must effectively detect undesirable performance behaviours, identify potential root causes, and take adequate corrective measures. The problem of uncovering and understanding performance anomalies and their causes (bottlenecks) in different system and application domains is well studied. In order to assess progress, research trends, and identify open challenges, we have reviewed major contributions in the area and present our findings in this survey. Our approach provides an overview of anomaly detection and bottleneck identification research as it relates to the performance of computing systems. By identifying fundamental elements of the problem, we are able to categorize existing solutions based on multiple factors such as the detection goals, nature of applications and systems, system observability, and detection methods.

B) *Detection of Performance Anomalies in Web-based* Applications

Performance management and dependability are two of the fundamental issues in business-critical applications. The ability to detect the occurrence of performance failures and anomalies has raised the attention of researchers in the last years. It is in fact a difficult problem, since a visible change in the performance can result from some natural cause (e.g., workload variations, upgrades) or by some internal anomaly or fault that may end up in a performance failure or application crash. Distinguish between the two scenarios is the goal of the framework presented in this paper. Our framework is targeted for web-based and component-based applications. It makes use of AOP-based monitoring, data correlation techniques and time-series alignment algorithms to spot the occurrence of performance anomalies avoiding false alarms due to workload variations. The paper includes some experimental results that show the effectiveness of our techniques under the occurrence of dynamic workloads and some fault-load situations.

C) *Root-cause analysis of performance anomalies in web-based applications*

The complexity behind current business-critical applications leads many times to performance problems difficult to anticipate and analyze. In our previous work we described a framework for detection of performance anomalies in webbased and component-based applications. It provides low overhead monitoring, correctly distinguishes performance anomalies from common workload variations and also presents initial information for system or application server changes related with an application performance anomaly. In this paper we present a framework extension devised to offer root-cause failure analysis for a given performance anomaly. The monitoring module enables application profiling and ANOVA analysis is used to verify if a performance anomaly is due to internal changes within the application (e.g., application updates) or to external changes (e.g., remote services changes, system/application server change). The paper includes some experimental results that show the effectiveness of our approach to pinpoint the root-cause for different types of performance anomalies and remarks its potential to avoid a considerable number of service failures.

D) *Detecting Abnormal Machine Characteristics in Cloud Infrastructures*

In the cloud computing environment resources are accessed as services rather than as a product. Monitoring this system for performance is crucial because of typical pay-per- use packages bought by the users for their jobs. With the huge number of machines currently in the cloud system, it is often extremely difficult for system administrators to keep track of all machines using distributed monitoring programs such as Ganglia1 which lacks system health assessment and summarization capabilities. To overcome this problem, we propose a technique for automated anomaly detection using machine performance data in the cloud. Our algorithm is entirely distributed and runs locally on each computing machine on the cloud in order to rank the machines in order of their anomalous behavior for given jobs. There is no need to centralize any of the performance data for the analysis and at the end of the analysis, our algorithm generates error reports, thereby allowing the system administrators to take corrective actions. Experiments performed on real data sets collected for different jobs validate the fact that our algorithm has a low overhead for tracking anomalous machines in a cloud infrastructure.

E) *Mining Modern Repositories with Elasticsearch*

Organizations are generating, processing, and retaining data at a rate that often exceeds their ability to analyze it effectively; at the same time, the insights derived from these large data sets are often key to the success of the organizations, allowing them to better understand how to solve hard problems and thus gain competitive advantage. Because this data is so fast-moving and voluminous, it is increasingly impractical to analyze using traditional offline, read-only relational databases. Recently, new "big data" technologies and architectures, including Hadoop and NoSQL databases, have evolved to better support the needs of organizations analyzing such data. In particular, Elasticsearch — a distributed full-text search engine — explicitly addresses issues of scalability, big data search, and performance that relational databases were simply never designed to support. In this paper, we reflect upon our own experience with Elasticsearch and highlight its strengths and weaknesses for performing modern mining software repositories research.

III. SYSTEM MODEL

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met:

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user;
2) The third party auditing process should bring in no new vulnerabilities towards user data privacy

a) Disadvantages

The existing system mainly focuses on detecting the unwanted anomalies at presented in the cloud platform applications it also detect the bottlenecks at occurs in the application it has successfully discovered the anomalies and bottlenecks using various algorithms and procedures But it failed to provide an solution to overcome the above mentioned anomalies. So only detecting is useful for identification purpose only so to overcome the above issues a new system should be build by keeping all requirements in mind.

b) Proposed System

In this work, we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users.

IV. PROPOED SYSTEM IMPLEMENTATION

To enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol design should achieve the following security and performance guarantee.

Public Auditing

To allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users.

Storage correctness

To ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact.

Privacy-preserving

To ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process.

Batch auditing

To enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

Lightweight

To allow TPA to perform auditing with minimum communication and computation overhead.

a) PROCESS OF TPA

The user should first login to the application. If the user in a new user then register him/her self to the application with the required details. Our application contains three login credentials they are the admin login, users login and tpa login. The admin login is the chief controller of our application because only the privileged person will be administrator. The users login will be the end users login who will use our application. The Tpa login is an inbuilt additional login provided by our system the administrator will provide all access to person who acts as tpa for the system. Our system mainly depends on resource allocation concepts of cloud computing so while the user's registration time the system will allocate the storage to the user based upon their requirement. The user cannot use the resource above their limit. Our system will efficiently calculate the resource consumed and displays the remaining availability of the resource at each time of consumption. So after the successful completion of utilization of the resource the user can download their uploaded file whenever they wanted so the process of tpa involves here For better security our system will not provide direct download of users data from the user. To download a data the user have to first send request to the TPA admin. Then the Tpa should accept the request that given by the user. Only after the successful acceptance of the request the user can download the data from the server. In addition to the provided security the user can download the data only after providing the random access code that was generated through inbuilt algorithm obtaining it from our mysql Database.

b) Homomorphic Authentication

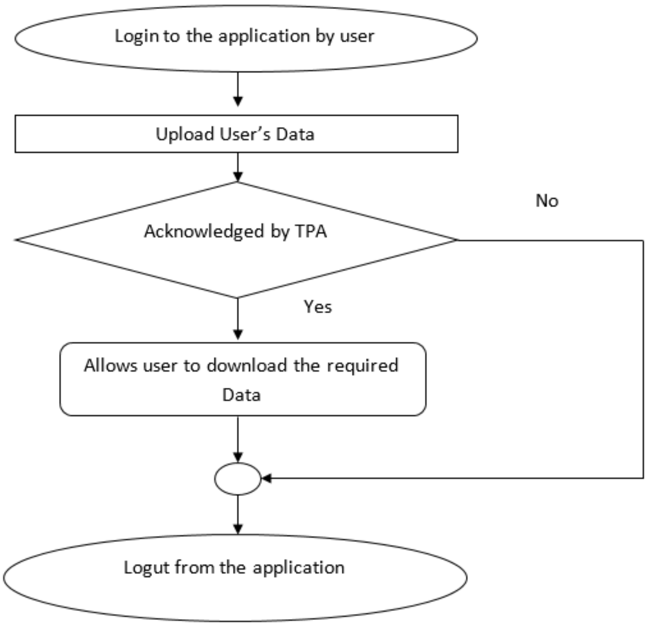
It is a form of encryption that permits users to perform computations on its encrypted data without first decrypting it. These resulting computations are left in an encrypted form which, when decrypted, result in an identical output to that produced had the operations been performed on the unencrypted data. Homomorphic encryption can be used for privacy-preserving outsourced storage and computation. This allows data to be encrypted and out-sourced to commercial cloud environments for processing, all while encrypted.

For sensitive data, such as health care information, homomorphic encryption can be used to enable new services by removing privacy barriers inhibiting data sharing or increase security to existing services. For example, predictive analytics in health care can be hard to apply via a third party service provider due to medical data privacy concerns, but if the predictive analytics service provider can operate on encrypted data instead, these privacy concerns are diminished.

Moreover, even if the service provider's system is compromised, the data would remain secure.

c) Cloud Auditing

A cloud auditor is a party that can perform an independent examination of cloud service controls with the intent to express an opinion thereon. Audits are performed to verify conformance to standards through review of objective evidence. A cloud auditor can evaluate the services provided by a cloud provider in terms of security controls, privacy impact, performance, etc. Auditing is especially important for federal agencies as “agencies should include a contractual clause enabling third parties to assess security controls of cloud providers”.


Login to the application by user
Upload User’s Data
Acknowledged by TPA
No
Yes
Allows user to download the required Data
Logut from the application

a) Login Page

The Home page consists of, Admin Login, User’s Login, TPA Login

b) Admin Login

The Administrator login is the chief controller of our application the admin panel has all the features of our application which includes then data upload section, verification section like all activities.

c) User’s Login

This login is made for the end users of our application for their major activities like uploading their data, downloading their data and verifying what data they had stored in their cloud storage.

V. CONCLUSION

The cloud computing applications has various numbers of advantages it also suffers from some numbers of disadvantages one of it is the resource allocation the process of allocating the resource available on the cloud to the needed users at the time of request it is a tedious process when the number of request for the resources increases so the performance increased resource allocation system has provided a solution by addition of an in-built third party auditing works to audit and provide the resource efficiently to the user at time of request.

In the Proposed system, the third party auditing was provided based on privacy preserving to securely store on cloud system and also provided batch auditing for efficient handling of the multiple users. In Future, the cloud platform will be used to store them. Various additional modules like crystal clear report generation for the users will be provided for the better awareness of their resources Then the public auditing can be used to bring new feature like no involvement of the service level agreement issusses between the consumers who consumes their resources and service providers.

VI. REFERENCES

[1]. O. Ibidunmoye, F. Herna´ndez-Rodriguez, and E. Elmroth, “Performance anomaly detection and bottleneck identification,” ACM Comput. Surv., vol. 48, no. 1, pp. 4:1–4:35, Jul. 2015. [Online].Available: http://doi.acm.org/10.1145/2791120

[2]. J. P. Magalhaes and L. M. Silva, “Detection of performance anomalies in web-based applications,” in Proceedings of the 2010 Ninth IEEE International Symposium on Network Computing and Applications, ser. NCA ’10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 60–67. [Online]. Available: http://dx.doi.org/10.1109/NCA.2010.15

[3]. J. a. P. Magalha˜es and L. M. Silva, “Root-cause analysis of performance anomalies in web-based applications,” in Proceedings of the 2011 ACM Symposium on Applied Computing, ser. SAC ’11. New York, NY, USA: ACM, 2011, pp. 209–216. [Online]. Available: http://doi.acm.org/10.1145/1982185.1982234

[4]. K. Bhaduri, K. Das, and B. L. Matthews, “Detecting abnormal machine characteristics in cloud infrastructures,” in 2011 IEEE 11th International Conference on Data Mining Workshops. IEEE, 2011, pp.137–144.

[5]. O. Kononenko, O. Baysal, R. Holmes, and M.W. Godfrey, “Mining modern repositories with elasticsearch,” in Proceedings of the 11thWorking Conference on Mining Software Repositories, ser. MSR 2014.New York, NY, USA: ACM, 2014, pp. 328–331. [Online]. Available:http://doi.acm.org/10.1145/2597073.2597091

[6]. Lu, X., Liao, Y., Lio, P. and Hui, P., 2020. Privacy-preserving asynchronous federated learning mechanism for edge network computing. IEEE Access, 8, pp.48970-48981.

[7]. Henze, M., 2020, June. The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation. In 2020 IEEE Conference on Communications and Network Security (CNS) (pp. 1-5). IEEE.

[8]. Manasrah, A.M., Shannaq, M.A. and Nasir, M.A., 2020. An investigation study of privacy preserving in cloud computing environment. Handbook of computer networks and cyber security, pp.43-61.

[9]. Kocabas, O. and Soyata, T., 2020. Towards privacy-preserving medical cloud computing using homomorphic encryption. In Virtual and Mobile Healthcare: Breakthroughs in Research and Practice (pp. 93-125). IGI Global.

[10]. Fan, Y., Bai, J., Lei, X., Zhang, Y., Zhang, B., Li, K.C. and Tan, G., 2020. Privacy preserving based logistic regression on big data. Journal of Network and Computer Applications, 171, p.102769.

[11]. Li, Y., Li, H., Xu, G., Xiang, T., Huang, X. and Lu, R., 2020. Toward Secure and Privacy-Preserving Distributed Deep Learning in Fog-Cloud Computing. IEEE Internet of Things Journal, 7(12), pp.11460-11472.

[12]. Tan, Y., Wu, W., Liu, J., Wang, H. and Xian, M., 2020. Lightweight edge-based kNN privacy-preserving classification scheme in cloud computing circumstance. Concurrency and Computation: Practice and Experience, 32(19), p.e5804.

[13]. Feng, J., Yang, L.T., Zhang, R., Qiang, W. and Chen, J., 2020. Privacy preserving high-order bi-lanczos in cloud-fog computing for industrial applications. IEEE Transactions on Industrial Informatics.

[14]. Huang, Q., Zhang, Z. and Yang, Y., 2020. Privacy-preserving media sharing with scalable access control and secure deduplication in mobile cloud computing. IEEE Transactions on Mobile Computing.

[15]. Jiang, M. and Yang, H., 2020. Secure outsourcing algorithm of BTC feature extraction in cloud computing. IEEE Access, 8, pp.106958-106967.

[16]. Wang, X., Gu, B., Qu, Y., Ren, Y., Xiang, Y. and Gao, L., 2020, June. Reliable customized privacy-preserving in fog computing. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.

Cite this article as :

Janakiraman M, Bala Murali Krishnan J, Nickelson S, Nihas Ahamed I, Ms. K.Veena, "Increased Performance In Resource Allocation System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 2, pp. 425-431, March-April 2021.
Journal URL : https://ijsrcseit.com/CSEIT2172105