International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Volume.06, Issue.01,
January-June, 2018,
Pages:0121-0123

MMBCloud-Tree: Authenticated Index for Verifiable Cloud Service Selection

K. VIJAYA LAKSHMI[1], K. SUNIL KUMAR[2]
[1]PG Scholar, Dept of CSE, DJR Institute of Engineering & Technology, Andhrapradesh, India,
E-mail: vijayalakshmikolusu90@gmail.com.
[2]Associate Professor, Dept of CSE, DJR Institute of Engineering & Technology, Andhrapradesh, India,
E-mail: sunil_ketineni@yahoo.co.in.

Abstract: Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. However, existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted, and do not provide any guarantee over the correctness of the service recommendations. It is then possible for a compromised or dishonest broker to easily take advantage of the limited capabilities of the clients and provide incorrect or incomplete responses. To address this problem, we propose an innovative Cloud Service Selection Verification (CSSV) scheme and index structures (MMBcloud-tree) to enable cloud clients to detect misbehavior of the cloud brokers during the service selection process. We demonstrate correctness and efficiency of our approaches both theoretically and empirically.

Keywords: Cloud Service Selection, Brokerage System, Merkle Hash Tree, Verification.

I. INTRODUCTION

This has resulted in a large number of cloud service providers (CSPs), offering a wide range of resources. The availability of various, possibly complex options, however, makes it difficult for potential cloud clients to weigh and decide which options suit their requirements the best. The challenges are twofold: 1) It is hard for cloud clients to gather information about all the CSPs available for their selections; 2) It is also computationally expensive to choose a suitable CSP from a potentially large CSP pool. In light of these difficulties, both industry and academia (see for a survey) suggested introducing an additional computing layer(referred to as cloud brokerage systems)on top of the base service provisioning to enable tasks such as discovery, mediation and monitoring. In a cloud brokerage system, one of the most fundamental tasks is to provide high-quality selection services for clients. That is, a broker provides clients with a list of recommended CSPs that meet the clients' needs. With the aid of cloud brokers, clients no longer need to collect, search or compare CSPs' services and capabilities. Without the ability to verify the correctness of the service recommendation, cloud clients could be easily cheated by malicious brokers. For instance, malicious brokers could recommend their favorable CSPs as much as possible and ignore other suitable CSPs, without being caught by the clients. More seriously, due to the lack of super vision and verification of brokers' actions, malicious brokers could even recommend malicious CSPs which collect and sell clients' private resources, monitor clients' hosts during cloud service provisioning, causing major financial and confidentiality losses to the clients. Therefore, it is important to equip the clients with verification capabilities of the obtained recommendations. The clients may not need to verify each recommendation result, but they certainly need to have the ability to do so when they feel necessary.

II. EXISTING SYSTEM

Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. However, existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted, and do not provide any guarantee over the correctness of the service recommendations. It is then possible for a compromised or dishonest broker to easily take advantage of the limited capabilities of the clients and provide incorrect or incomplete responses. To address this problem.

III. PROPOSED SYSTEM

We propose an innovative Cloud Service Selection Verification (CSSV) scheme and index structures (MMB cloud-tree) to enable cloud clients to detect misbehavior of the cloud brokers during the service selection process. We demonstrate correctness and efficiency of our approaches both theoretically and empirically as shown in Fig.1. Proposed a new performance measuring method for Infrastructure-as-Service offerings, taking into account the type of services running in a virtual machine. Presented a framework for monitoring cloud performance based on customers' feedback. Li and Wang in addition proposed a probability method to evaluate the subjective trustworthiness of the service component as well as the whole composite service from a series of ratings given by customers. The range tree-based method proposed in needs to build and embed a Merkle hash tree for each node, and. this process is also recursively invoked for the nodes of the embedded Merkle hash tree, which makes index contruction, querying and verification extremely time consuming; the VB-tree in is not efficient for queries on non-key properties because it will generate large size proof messages to cover the nodes in-between the query ranges but do not contain the query results.

Copyright @ 2018 IJIT. All rights reserved.

X`Han et al. described a recommendation system in cloud computing suitable for design-time decisions as it statically provided a ranking of available cloud providers. Li et al. developed systematic comparator CloudCmp to help customers choose a cloud that meets their needs through measuring and comparing the elastic computing, persistent storage and networking services

Algorithm:

- **Verification Algorithms:** It is worth noting that, the novelty of our approaches not only lies in a new set of verification algorithms specific to the cloud service selection, but also gives efficient solutions (compared with the state-of-the-art) to the problem of authenticating multidimensional queries.
- **RSA Signing Algorithm:** RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of an integer is hard (the factoring problem).

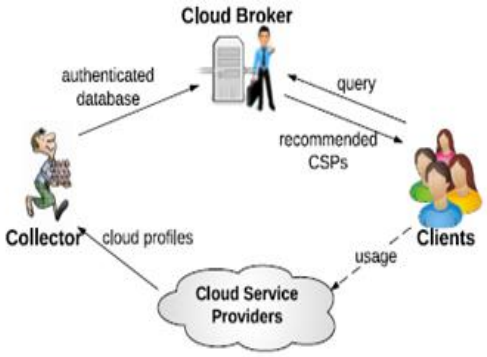

Fig.1. System Architecture.

IV. RELATED WORK

- Cloud service selection,
- Brokerage system
- Verification
- Merkle Hash Tree

A. Cloud Service Selection

It is worth noting that, the novelty of our approaches not only lies in a new set of verification algorithms specific to the cloud service selection, but also gives efficient solutions (compared with the state-of-the-art) to the problem of authenticating multidimensional queries. The reason to choose Price as the indexing field is two-fold. First, given that most cloud providers employ a pay-per-use business model, Price is one of the most commonly occurred criteria in cloud service selection queries. First, cloud service selection typically allows cloud users to specify multiple service requirement is always desirable to have efficient cloud service selection and verification so that the cloud end users would not feel delay of services. Our novel index structure is the core component of our Cloud Service Selection Verification (CSSV) scheme, which employs the idea of "separation of duties" to ensure strong security guarantees. we propose the Cloud Service Selection Verification (CSSV) scheme which is a comprehensive solution that is capable of guaranteeing all the three security requirements (i.e., authenticity, satisfiability and completeness).

B. Brokerage System

In a cloud brokerage system, one of the most fundamental tasks is to provide high-quality selection services for clients. That is, a broker provides clients with a list of recommended CSPs that meet the clients' needs. With the aid of cloud brokers, clients no longer need to collect, search or compare CSPs' services and capabilities Precisely, we introduce a trusted collector in the cloud brokerage system that separates the task of CSP information collection from the service selection. The collector does not directly interact with the cloud clients and is only in charge of gathering information from the CSPs, and hence it can be more devoted into adopting sophisticated defenses to filter out problematic data and building an authenticated database of CSPs' profiles.

C. Verification

More seriously, due to the lack of supervision and verification of brokers' actions, malicious brokers could even recommend malicious CSPs which collect and sell clients' private resources, monitor clients' hosts during cloud service provisioning, causing major financial and confidentiality losses to the clients. we propose innovative authenticated index structures and verification protocols to allow clients to verify the completeness and authenticity of brokers' answers. This problem is related to that of authentication of query results for outsourced databases. selection and verification so that the cloud end users would not feel delay of services, but existing few works , although support authentication of multi-dimensional query results, are time consuming, resulting that they could not meet the demands of today's real-time cloud service recommendations.

D. Merkle Hash Tree

This process is also recursively invoked for the nodes of the embedded Merkle hash tree, which makes index contruction, querying and verification extremely time consuming; the VB-tree in is not efficient for queries on non-key properties because it will generate large size proof messages to cover the nodes in-between the query ranges but do not contain the query results. The leaf nodes in the Merkle hash tree contain the hash values of the original data items. Each internal node contains the hash value of the concatenation of the hash values of its two children nodes. The hash value of the root of the tree is published for verification. If there is any change to the original data values, one would not be.

V. CONCLUSION

In this paper, we presented an innovative Cloud Service Selection Verification (CSSV) system to achieve cheating-free cloud service selection under a cloud brokerage architecture. The core of our system is an efficient authenticated index structure to ensure the authenticity, the

satiability and the completeness of the service selection results. Our theoretical and experimental results demonstrate the effectiveness and efficiency of our schemes compared with the state-of-the-art. As part of our future work, we plan to consider a verifiable scheme for best service selection query whereby the broker returns only the best CSP instead of all candidate CSPs with respect to a client's request.

VI. RESULTS

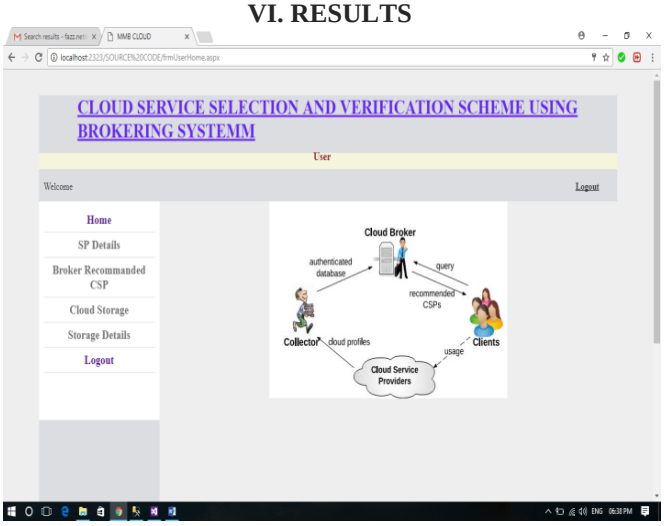

Fig.2.

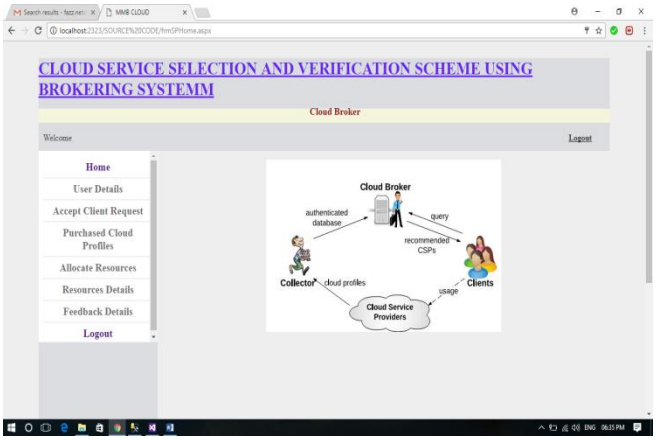

Fig.3.

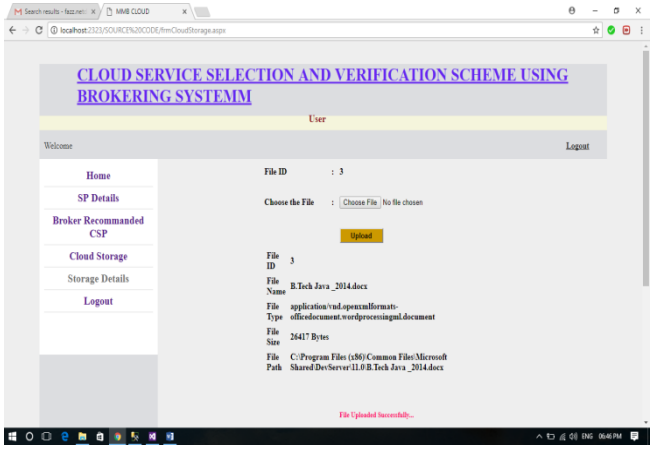

Fig.4.

VII. REFERENCES

[1] Y. Chen, V. Paxson, and R. H. Katz, "What's new about cloud computing security," EECS Dept., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2010-5, Jan. 20, 2010.

[2] S. K. Habib, S. Ries, and M. Muhlhauser, "Towards a trust management system for cloud computing," in Proc. IEEE 10th Int. Conf. Trust, Secur. Privacy Comput. Commun., 2011, pp. 933–939.

[3] K. M. Khan and Q. Malluhi, "Establishing trust in cloud computing," IT Prof., vol. 12, no. 5, pp. 20–27, Oct. 2010.

[4] J. Lin, C. Chen, and J. Chang, "Qos-aware data replication for data intensive applications in cloud computing systems," IEEE Trans. Cloud Comput., vol. 1, no. 1, pp. 101–115, Jan.–Jun. 2013.

[5] D. Gambetta, "Can we trust trust?" in Trust: Making and Breaking Cooperative Relations, D. Gambetta, Ed. Oxford, U.K.: Blackwell, 1990, ch. 13, pp. 213–237.

[6] D. H. Mcknight and N. L. Chervany, "The meanings of trust," Manage. Inf. Syst. Res. Center, Univ. Minnesota, Minneapolis, MN, USA, Tech. Rep. MISRC Working Paper Series 96 04, 1996.

[7] D. Manchala, "Trust metrics, models and protocols for electronic commerce transactions," in Proc. 18th Int. Conf. Distrib. Comput. Syst., 1998, pp. 312–321.

[8] A. Jøsang and S. L. Presti, "Analysing the relationship between risk and trust," in Proc. 2nd Int. Conf. Trust Manage., Mar. 2004, pp. 135–145.

[9] L. Freeman, "Centrality on social networks," Social Netw., vol. 1, pp. 215–239, 1979.

[10] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Commun. Surv. Tutorials, vol. 3, no. 4, pp. 2– 16, Fourth Quarter 2000.

[11] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," Decision Support Sys., vol. 43, no. 2, pp. 618–644, Mar. 2007.

[12] P. Resnick and R. Zeckhauser, "Trust among strangers in internet transactions: Empirical analysis of ebay's reputation system," in The Economics of the Internet and ECommerce, series Advances in Applied Microeconomics, vol. 11, M. Baye, Ed. Amsterdam, The Netherlands: Elsevier, 2002, pp. 127–157.

Author's Profile:

K. Vijaya Lakshmi received her B.Tech degree in Computer Science & Engineering and pursuing M.Tech degree in computer science and engineering from , DJR Institute of Engineering & Technology.

K. Sunil Kumar M.Tech received his M.Tech degree and B.Tech degree in Computer Science & Engineering. he is currently working as an Assoc Professor in DJR Institute of Engineering & Technology.