ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

Intelligent Cloud Service Selection Using Multi-Merkle B-Cloud Tree Strategies

K.Saru Nivedha[1], P.Ponvasan[2]

M.E. Computer Science and Engineering, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Karaikudi, TamilNadu, India.

Assistant Professor, Department of Computer Science and Engineering, Sri Raaja Raajan College of Engineering and Technology, Amaravathipudur, Karaikudi, TamilNadu, India.

ABSTRACT: The main motto of this system is to provide the trusted cloud and easily accessible environment to users to maintain and retrieve their data in more efficient manner. Multi-Merkle Bcloud Tree infrastructure is used in this system for trusted data maintenance. Cloud Service Provider (CSP) is responsible for all transactions into the cloud environment, but that CSP doesn't have an ability to check other's data presented into the cloud. End-to-End Security is highly concentrated via integrated Authentication methodologies. Cloud brokers have been recently introduced as an additional computational layer to facilitate cloud selection and service management tasks for cloud consumers. But existing brokerage schemes on cloud service selection typically assume that brokers are completely trusted and do not provide any guarantee over the services. For all in this system users can securely maintain and retrieve the data without any interruptions.

KEYWORDS: MMB, MMB Cloud, Cloud service selection, brokerage system, Merkle hash tree, verification

I. INTRODUCTION

Cloud Services offer a scalable variety of storage space and computing capabilities, which are widely employed by an increasing number of business owners. 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 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.

The underlying assumption in the existing cloud brokerage schemes is that brokers are completely trusted and thus will always provide unbiased best available options to clients. Under this assumption, none of the existing works provides guarantees over the correctness or completeness of the service selection recommendations to the cloud clients. 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 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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

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. In this work, we propose innovative authenticated index structures and verification protocols to allow clients to verify the completeness and authenticity of brokers' answers.

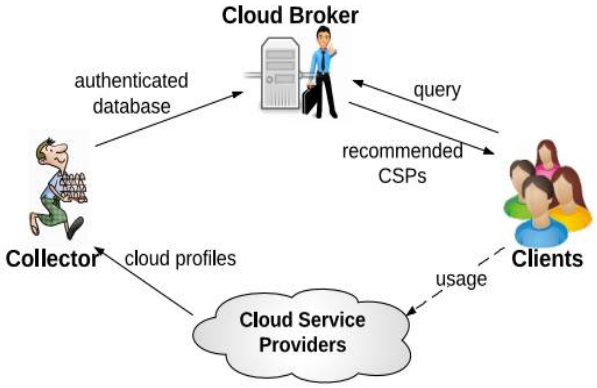

Fig.1 Proposed System Architecture

This problem is related to that of authentication of query results for outsourced databases. However, the characteristics of cloud service selection actually raise a new series of challenges. First, cloud service selection typically allows cloud users to specify multiple service requirements (i.e., multi-dimensional range queries), whereas many existing works on query authentication only support range queries on one or two dimensions (e.g., verifying location-based query results). Second, it is always desirable to have efficient cloud service 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.

In order to overcome the limitations of existing techniques, both in terms of efficiency and supported functionality, we propose a new authenticated index structure, called Multi-Merkle Bcloud-tree (MMBcloud-tree), which is a variant of the Merkle B+-tree and is specifically tailored for cloud service selections. In particular, we first design the Merkle Bcloud-tree (MBcloud-tree) which is an authenticated index on the most common property (i.e., Price) of CSPs, and propose the corresponding verification protocol. Then, we extend the MBcloud-tree to the MMBcloud-tree by integrating a multi-dimensional indexing method (i.e., iDistance) with MBcloud-tree, to further improve the selection quality as well as reduce the verification burden at the client side. Our approaches are proved to ensure authenticity, satisfiability and completeness of the selected results. We have also experimentally compared our approaches with the most recent related work, and the results demonstrate significant improvements over the state-of-the-art.

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. 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. The collector is allowed to make profit by selling the authenticated database to one or more cloud brokers. With the available authenticated databases, the cloud brokers focus on handling probably a large number of real-time service requests from clients.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

II. EXISTING APPROACHES – A SUMMARY

Cloud Services offer a scalable variety of storage space and computing capabilities, which are widely employed by an increasing number of business owners. 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 dif- ficult for potential cloud clients to weigh and decide which options suit their requirements the best. The challenges are twofold: (a) It is hard for cloud clients to gather information about all the CSPs available for their selections and (b) It is also computationally expensive to choose a suitable CSP from a potentially large CSP pool. Existing works on cloud service selection are focused only on how to select the services that satisfy customers' requirements. None of them considers security issues involved in the service selection, and none of them provides verifiable schemes to prove the correctness and completeness of their service selection results as addressed in our work. The existing system contains the following disadvantages, they are listed as follows: (a) Fully Broker based data maintenance methodology and data are open to server administrator, (b) Existing works on cloud service selection are focused only on how to select the services that satisfy customers' requirements and (c) None of them considers security issues involved in the service selection, and none of them provides verifiable schemes to prove the correctness and completeness of their service selection results as addressed in our work.

III. PROPOSED SYSTEM SUMMARY

Existing use the collector for securely generating and sharing location-based information, whereas we use the collector to achieve service verification in the cloud. Our proposed authenticated index structures are related to those developed for query authentication in outsourced databases which can be classified into two main categories: Hash-based approaches and Signature-based approaches. As our proposed data structure is developed based on the Merkle hash tree. The proposed system contains the following advantages, they are listed as follows: (a) Broker free trusted data maintenance service, (b) CSP cannot able to view the Server data and (c) Cost, Time and Performance is so effective.

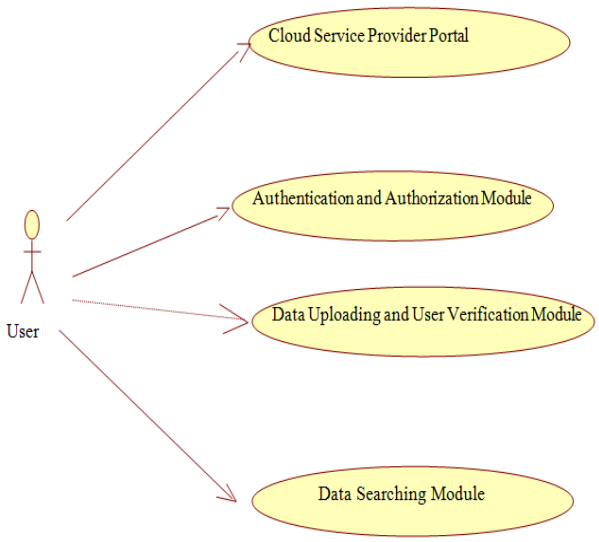

Fig.2 UseCase Diagram

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

IV. SYSTEM IMPLEMENTATION

The proposed system is designed with lots of purposeful modules that are described in detail:

A. Cloud Service Provider Portal

This Cloud Service Provider Portal module is the Main Portal for Cloud Service Provider, which provides an ability to the CSP to navigate to the respective pages such as Cloud Server Creation, Registration Accept/Removal and File Maintenance Portal. Generally says, a cloud Service provider is a company or individual, which offers some component of cloud computing – typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) – to other businesses or individuals. Cloud providers are sometimes referred to as cloud service providers or CSPs.

B. Authentication and User Verification Module

Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. User authentication is the verification of an active human-to-machine transfer of credentials required for confirmation of a user's authenticity; the term contrasts with machine authentication, which involves automated processes that do not require user input.

The User Verification Module is to easily configure permissions and anything else; the verification process is role-based. New users optionally obtain a quarantine role, which can be used for evaluation, observation or simply for confusion and ambiguities. This module allows you to have e-mail verification and in meanwhile allowing the users to type their own passwords. If they do not verify their accounts in a certain time interval the user will be blocked.

C. Data Uploading and Cloud Broker Authorization

This Data Uploading module allows the data owner to upload the data into Cloud Server without any security issues. It allows the data owner to maintain their files into server with proper descriptions. Uploading is the transmission of a file from one computer system to another, usually larger computer system. From a network user's point-of-view, to upload a file is to send it to another computer that is set up to receive it.

Cloud Broker Authorization module allows the brokers to register their identities into the system with proper nature. Cloud access security brokers (CASBs) are on-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, and malware detection/prevention and so on.

D. Data Searching Portal

The module of Data Searching allows the data user to search for the required data from the cloud and get access from the server immediately with proper security norms. This portal is efficient for searching the data from server with advanced content based searching mechanisms.

V. LITERATURE SURVEY

In the year of 2012, the authors "K. Ren, C.Wang, Q.Wang et al." proposed a paper titled "Security challenges for the public cloud", in that they described such as: Cloud computing represents today's most exciting computing paradigm shift in information technology. However, security and privacy are perceived as primary obstacles to its wide adoption. Here, the authors outline several critical security challenges and motivate further investigation of security solutions for a trustworthy public cloud environment.

In the year of 2010, the authors "S. Kamara and K. Lauter" proposed a paper titled "Cryptographic cloud storage in Financial Cryptography and Data Security", in that they described such as: the problem of building a secure cloud storage service on top of a public cloud infrastructure where the service provider is not completely trusted by the customer. We describe, at a high level, several architectures that combine recent and non-standard cryptographic

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

primitives in order to achieve our goal. We survey the benefits such an architecture would provide to both customers and service providers and give an overview of recent advances in cryptography motivated specifically by cloud storage.

In the year of 2010, the authors "O. Goldreich and R. Ostrovsky" proposed a paper titled “Software Protection and Simulation on Oblivious Rams", in that they described such as: Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection.

We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in which it accesses memory locations is equivalent for any two inputs with the same running time. For example, an oblivious Turing Machine is one for which the movement of the heads on the tapes is identical for each computation. (Thus, the movement is independent of the actual input.) What is the slowdown in the running time of a machine, if it is required to be oblivious? In 1979, Pippenger and Fischer showed how a two-tape oblivious Turing Machine can simulate, on-line, a one-tape Turing Machine, with a logarithmic slowdown in the running time.

We show an analogous result for the random-access machine (RAM) model of computation. In particular, we show how to do an on-line simulation of an arbitrary RAM by a probabilistic oblivious RAM with a polylogaithmic slowdown in the running time. On the other hand, we show that a logarithmic slowdown is a lower bound.

VI. EXPERIMENTAL RESULTS

The following figure shows the home page of the proposed system.

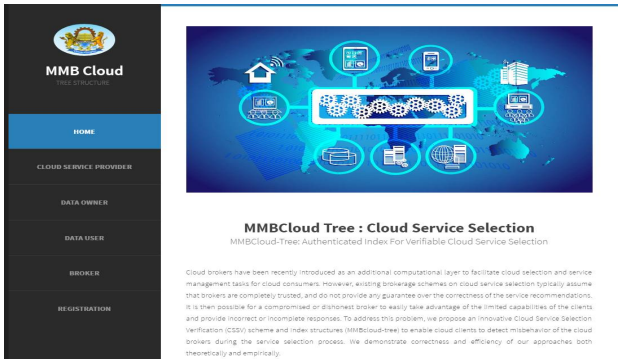

Fig.3 Home Page

The following figure illustrates the new user registration details of the proposed system.

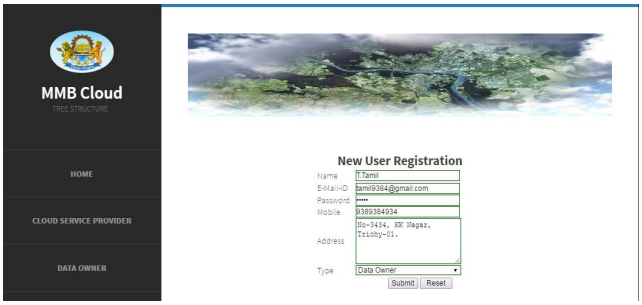

Fig.4 New User Registration

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

The following figure illustrates the CSP Authentication Details of the proposed system.

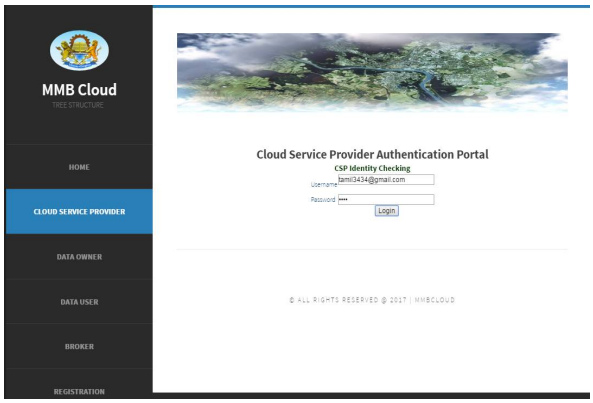

Fig.5 CSP Authentication

The following figure illustrates the Cloud Service Creation Details of the proposed system.

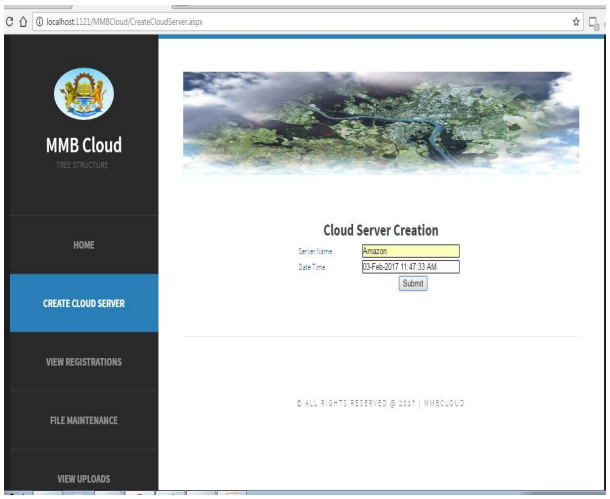

Fig.6 Cloud Service Creation

VII. CONCLUSION

In this system, we propose an innovative Cloud Service Selection Verification (CSSV) system to achieve cheating-free cloud service selection under cloud brokerage architecture. The core of our system is an efficient authenticated index structure to ensure the authenticity, the satisfiability and the completeness of the service selection results. Our experimental results show the effectiveness and efficiency of our schemes compared with the state-of-the-art.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 2, February 2018

REFERENCES

[1] I. Petri, M. Punceva, and O. F. Rana, "Broker emergence in social slouds," 2013 6th International Conference on Cloud Computing, pp. 669–676, 2013.
[2] A. Li, X. Yang, S. Kandula, and M. Zhang, "CloudCmp: comparing public cloud providers," in IMC '10: Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. New York, New York, USA: ACM Press, 2010, pp. 1–14.
[3] C. Binnig, D. Kossmann, T. Kraska, and S. Loesing, "How is the weather tomorrow?: towards a benchmark for the cloud," in DBTest '09: Proceedings of the Second International Workshop on Testing Database Systems. ACM Request Permissions, Jun. 2009.
[4] A. Lenk, M. Menzel, J. Lipsky, S. Tai, and P. Offermann, "What are you paying for? performance benchmarking for Infrastructure-as-a-Service offerings," in 2011 IEEE International Conference on Cloud Computing (CLOUD), 2011, pp. 484–491.
[5] Z. ur Rehman, O. K. Hussain, S. Parvin, and F. K. Hussain, "A framework for user feedback based cloud service monitoring," in 2012 Sixth International Conference on Complex, Intelligent and Software Intensive Systems (CISIS), 2012, pp. 257–262.
[6] L. Li and Y. Wang, "Subjective trust inference in composite services." AAAI, 2010.
[7] L. Qu, Y. Wang, and M. A. Orgun, "Cloud service selection based on the aggregation of user feedback and quantitative performance assessment," in 2013 IEEE International Conference on Services Computing (SCC), 2013, pp. 152–159.
[8] L. Xin and A. Datta, "On trust guided collaboration among cloud service providers," in 2010 6th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 2010, pp. 1–8.
[9] S. Sundareswaran, A. Squicciarini, and D. Lin, "A brokerage-based approach for cloud service selection," in 2012 IEEE 5th International Conference on Cloud Computing (CLOUD). IEEE, Aug. 2012, pp. 558–565.
[10] F. Li, M. Hadjieleftheriou, G. Kollios, and L. Reyzin, "Dynamic authenticated index structures for outsourced databases," in SIGMOD '06: Proceedings of the 2006 ACM SIGMOD international conference on Management of data. ACM Request Permissions, Jun. 2006.
[11] E. Mykletun, M. Narasimha, and G. Tsudik, "Signature bouquets: immutability for aggregated/condensed signatures," in Computer Security – ESORICS 2004, ser. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2004, vol. 3193, pp. 160–176.
[12] M. Narasimha and G. Tsudik, "DSAC: integrity for outsourced databases with signature aggregation and chaining," in Proceedings of the 14th ACM International Conference on Information and Knowledge Management, 2005, pp. 235–236.
[13] H. Pang, A. Jain, K. Ramamritham, and K.-L. Tan, "Verifying completeness of relational query results in data publishing," in Proceedings of the 2005 ACM SIGMOD International Conference on Management of Data, 2005, pp. 407–418.
[14] H. Pang, J. Zhang, and K. Mouratidis, "Scalable verification for outsourced dynamic databases," Proceedings of the VLDB Endowment, vol. 2, no. 1, pp. 802–813, 2009.
[15] Q. Zheng, S. Xu, and G. Ateniese, "Efficient query integrity for outsourced dynamic databases," in CCSW '12 Proceedings of the 2012 ACM Workshop on Cloud computing security workshop. ACM, 2012, pp. 71–82.