International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 05, May 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

MULTI-AUTHORITY ACCESS CONTROL OUTSOURCING PROGRAMMING USING CLOUD

Auote Akshay B[1], Sarika Hirve M[2], Jadhav Pallavi L[3], Jare Sonali K[4]

Asst Prof. Shital Kolte[5]

[1,2,3,4] *Department of Computer Engineering, GSMCOE Balewadi, Pune (India)*

[5]*Prof.Department of Computer Engineering, GSMCOE Balewadi, Pune (India)*

ABSTRACT

Internet computing technologies, like grid computing, enable a weak computational device connected to such a grid to be less limited by its inadequate local computational, storage, and bandwidth resources. However, such a weak computational device (PDA, smartcard, sensor, etc.) often cannot avail itself of the abundant resources available on the network because its data are sensitive. Cloud computing promises greater flexibility in business planning along with significant cost savings by leveraging economies of scale in the IT infrastructure. It also offers a simplified capital and expenditure model for compute services as well as increased agility for cloud customers who can easily expand and contract their IT services as business needs change . The main objective of cloud computing enables customers with limited computational resources to outsource their large computation workloads to the cloud, and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. One fundamental advantage of the cloud paradigm is computation outsourcing, where the computational power of cloud customers is no longer limited by their resource-constraint devices. Outsourcing is to store the task or data which user wants it to do from outside their system such as cloud. By outsourcing the workloads into the cloud, customers could enjoy the literally unlimited computing resources in a pay-per-use manner without committing any large capital outlays in the purchase of hardware. Large-scale problems in the physical and life sciences are being revolutionized by Internet computing technologies, like grid computing, that make possible the massive cooperative sharing of computational power, bandwidth, storage, and data. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Some approaches also offers a simplified capital and expenditure model for compute services as well as increased agility for cloud customers who can easily expand and contract their IT services as business needs change. As the most recent evolution in computing architecture, cloud computing is simply a further extension of the distributed computing model.

Keywords— Cloud computing, secure outsourcing, quadratic programming, KKT condition

International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 05, May 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

I. INTRODUCTION

Commoditized outsourced computing has finally arrived, mainly due to the emergence of fast and cheapnetworking and efficient large scale computing. Amazon, Google, Microsoft and Sun are just a few of theproviders starting to offer increasingly complex storage and computation outsourcing "cloud" services. CPU cycles have become consumer merchandise. The outsourcing concept incorporates a wide range of flavors. On the one hand, global-wide giants such as Google offer mostly managed "cloud" facilities as part of infrastructures composed of tens of thousands of nodes. At the other side of the spectrum we find a plethora of small and medium sized startups or more established companies such as RackSpace, Mosso, InetU, hosting.com, Verio, FastServers, and tens of others. These companies offer services ranging from simple, raw networked hardware hosting client-provided operating system images and/or applications to more complex infrastructure setups with specifically deployed and managed application servers ready to support clients' workloads. Current clouds seem to be well suited and cost-effective for personal and small enterprise clients that increasingly outsource data-driven web-based retail and end-user interfaces and minimize their in-house computing management footprints. Yet clouds have been somewhat less successful in attracting medium to large corporations. Such clients often fall under strict regulatory compliance requirements for manipulating information or simply are reluctant to place sensitive data and computation logic under the control of a remote, third-party provider, without practical assurances of privacy and confidentiality in which the provider is untrusted

1.1 PROBLEM STATEMENT

In the proposed research work to design and implement a system which will provide the data security from collusion attack in trusted as well un-trusted cloud environments. The system will focus long communication scenario between data owner, CA, user, TTP and authorities using different security techniques, it will provide highest security than all existing approaches. (Using Amazon EC2 VM Consol).

1.2 OBJECTIVES

- Security of Access Policy
- Security against collision attack
- Data confidentiality guarantee
- Soundness and completeness
- Security against Compromising Aas
- Robustness

.

II. EXISTING SYSTEM

In the system model of outsourcing computation, the customer is threatened by malicious behaviors of the cloud. As introducing, therear two cloud models inout sourcing computation: semi-honest model and malicious model. In semi-honest model, the cloud performs according to the protocol. But it intends to analyze the encrypted input and the out put produced by itself. It makes efforton not only performing computation, but also

ISSN (O) 2454-9665
ISSN (P) 2454-0663

learning sensitive information which should remain private. While the malicious cloud may deviate from the protocol and return arand omans werhoping not to be detected by the customer in the meanwhile. In this model, the customer is compelled to verify the result for the purpose of resisting the cloud's cheating behavior. In this paper, we take the malicious cloud model into consideration.

As illustrated there are two parties involved in the system model of outsourcing QP problem. One party is the customer who has a large-scale QP problem to solve. But constrained by its limited computing resource, the customerintend stout source the large-scale QP problemto the cloud. The other party is the cloud, who is equipped with powerful computing resources. The whole outsourcing processisillu strated as follows .First, to protect the inputprivacy, the customer encrypts the original QP problem 5 into an encryptedone5K withasecretKeyK.Then5K isdelivered from the customer to the cloud. The cloud runs optimization algorithm to solve 5K when receiving the encrypted QP problem 5K. Next, the cloud provides both the solution and an appended proof to the customer. After getting the result, the customer verifies whether the solution returned is correct or not in encryption domain. If the result cannot pass through verification, the customer claims the answer returned is wrong and requires the cloud to compute it again. Otherwise ,the cust omercangetthe ultimate optimal solution to the original QP problem by decrypting the correct result.

III. PROPOSED SYSTEM

Proposed methods the introduced Ciphertext approach quality based encryption framework, that proposed CP-ASBE which is a form of CP-ABE, which organizes user attributes into a recursive family of sets and also allows to users to establish dynamic constraints on how attributes may be combined. And also this system shows how CP-ASBE can support compound attributes, and numerical attributes with multiple those value assignments. In their work, design of CP-ASBE system is secure in the standard model but extending for a multi-authority system.

the full security by achieving the dual system encryption strategy. The main challenge of applying dual system encryption strategy to ABE is the structure of keys and Ciphertext. In IBE or HIBE system, structure of keys and ciphertexts are both associated with the same type of simple object that is identities. In this paper, author presents two completely secure useful encryption plans. Their first result is a completely secure property based encryption (ABE) plan.

system has single authority which can monitor every single attribute of all users is unrealistic. Therefore Multi-authority attribute-based encryption which enables a more realistic classification of attribute-based access control, such that the advantage is that different authorities are responsible for assigning different sets of attributes to users.

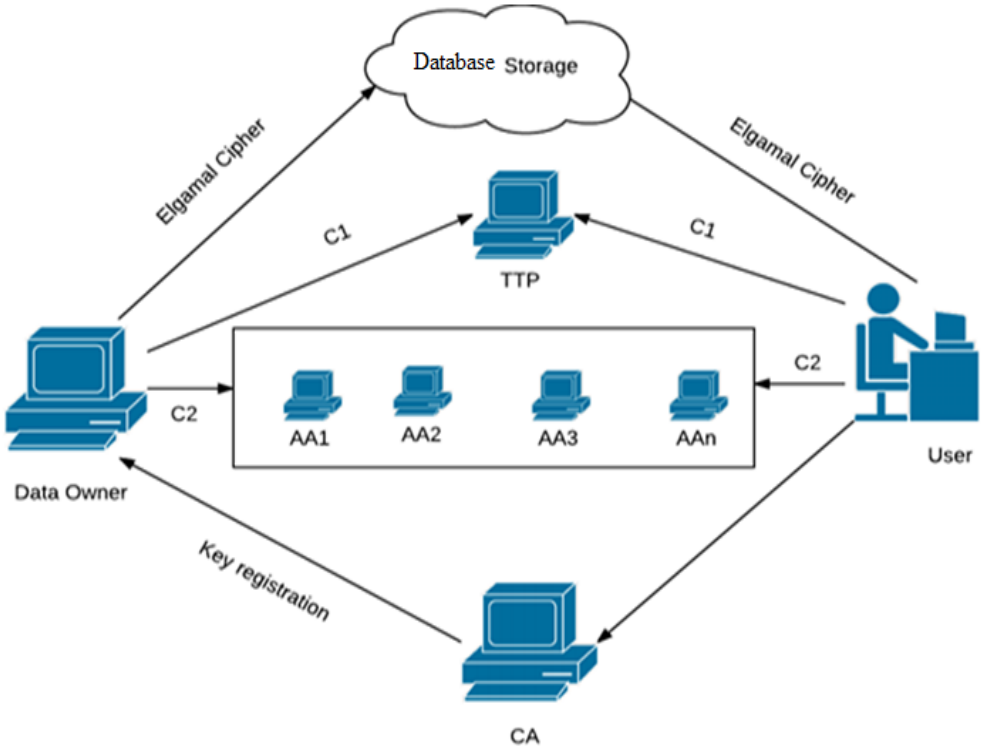
IV. IMPLEMENTATION

The research work focus on cloud data storage security, which has always been an most aspect of quality of service. For ensuring the correctness of cloud clients data in the cloud, in this paper propose an highly effective and flexible distributed scheme with two features, apposing to its predecessors. By using the homomorphic token with distributed verification of erasure coded data. In This paper proposed the integration of storage correctness insurance and data error localization most of works, the new scheme further supports secure and

ISSN (O) 2454-9665
ISSN (P) 2454-0663

efficient dynamic operation on data block including operations. We relies on erasure-correcting code in the file distribution preparation to support redundancy parity vectors for verification of erasure coded data using the homomorphic token, In this paper our scheme achieves the integration of data error localization and storage correctness insurance. This paper proposed highly effective and flexible distributed scheme with explicit dynamic data provide to ensuring the correctness of user‟ s data in the cloud. our scheme enable the data owner to delegate of data file re-encryption and user secret key update to cloud servers without disclosing data contents .In this paper we achieves this goal by exploiting and uniquely combing techniques that is token pre computation, error correctness verification as well as error localization and error recovery. In the first reason cryptography services for the intention of data security protection could not be directly adopted due to the users‟ loss control of data under cloud computing. So, verification of correct data storage in the must be conducted without explicit knowledge of the entire data. Assuming various kinds of data for every cloud client stored in the cloud and requirements of long term continuous assurance of their data safely, the problem is that verifying exactness of data storage in the cloud becomes even more challenging. This construction drastically decreasing the communication and storage overhead as compared to the based file of replication in distribution techniques. Therefore correctness of data and availability of the data being stored on the distributed cloud servers may be guaranteed. The key issues is to highly detect any unauthorized data alternation and corruption, possibly due to server compromise byzantine failure.

Fig.3.1. System conceptual flow



ISSN (O) 2454-9665
ISSN (P) 2454-0663

V. SYSTEM APPLICATION

- Public cloud base security application
- Document base privacy systems

VI. HARDWARE & SOFTWARE COMPONENTS

1.1 SOFTWARE REQUIREMENT:

Front End

- Jdk 1.7.0
- Internet Explorer 6.0/above
- Tool : Net Beans 7.4

Back-End

- MySQL 5.1

1.2 HARDWARE REQUIREMENT:

- Processor:- Intel Pentium 4 or above
- Memory:- 512 MB or above
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Other peripheral:- Printer
- Hard Disk:- 10gb

VII. CONCLUSION AND FUTURE SCOPE

8.1 CONCLUSION

In this review we then showed that deploying the cloud as a simple remote encrypted file system is extremely unfeasible if considering only core technology costs. Similarly, existing single server cryptographic oblivious data access protocols are not only time-impractical (this has been shown previously) but also (surprisingly) orders of magnitude more dollar expensive than trivial data transfer. Finally we concluded that existing secure outsourced data query mechanisms are mostly cost-unfeasible because today's cryptography simply lacks the expressive power to efficiently support outsourcing to untrusted clouds. Hope is not lost however. We were able to find borderline cases where outsourcing of simple range queries can break even when compared with local execution. These scenarios involve large amounts of outsourced data (e.g., 109 tuples) and extremely selective queries which return only an infinitesimal fraction of the original data (e.g., 0.00001%) – confirming the minimal CPU-intensive requirement principle on cloud feasibility. The scope did not permit us to explore the fascinating broader issues at the intersection of technology with business models, risk, behavioral incentives,

ISSN (O) 2454-9665
ISSN (P) 2454-0663

socio-economics, and advertising markets. We illustrate in a cloud computing setting, yet we (secretly) hope this type of reasoning will initiate a new current of practical, bottom-line aware designs of security protocols.

8.2 FUTURE SCOPE

The research work focus on cloud data storage security, which has always been an most aspect of quality of service. For ensuring the correctness of cloud clients data in the cloud, in this paper propose an highly effective and flexible distributed scheme with two features, apposing to its predecessors. By using the homomorphic token with distributed verification of erasure coded data. In This paper proposed the integration of storage correctness insurance and data error localization most of works, the new scheme further supports secure and efficient dynamic operation on data block including operations. We relies on erasure-correcting code in the file distribution preparation to support redundancy parity vectors for verification of erasure coded data using the homomorphic token, In this paper our scheme achieves the integration of data error localization and storage correctness insurance.

VIII. ACKNOWLEDGEMENT

We are deeply indebted to our seminar guide, Asst.Prof. ShitalKolte for his valuable guidance and support for completion of this seminar.

We are thankful to all our teachers and professors of our department for giving us their expertise in the related topic.

We would also like to thank our library staff, internet staff and laboratory assistants for providing us cordial support andnecessary facilities which were of great help for preparing this report.

IX. REFERENCES

[1] R. Bobba, H. Khurana, and M. Prabhakaran, “Attribute-sets: A practically moticated enhancement to attributebased encryption” 2009.

[2] Sahai and B. Waters, proposed the approach “Fuzzy identity-based encryption” 2005.

[3] Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attributebased encryption and (hierarchical) inner product encryption” 2005.

[4] N. Attarpadung, B. Libert, and E. Panafieu, ”Expressive keypolicy attribute-based encryption with constant-size ciphertexts,” in 2011.

[5] M. Chase and S. Chow, “Improving privacy and security in multi authority attribute-based encryption,” in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 121–130.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, “Achieving secure, scalable, and fine-grained data access control in cloud computing,” in INFOCOM’10. IEEE, 2010, pp. 534–542.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

[7] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in AsiaCCS'13.ACM, 2013, pp. 523–528.

[8] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE Trans. Info. Forensics Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[9] Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold MultiAuthority Access Control System in Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems,Vol. PP,Issue 99, pp.1-12, 2015.

[10] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, Vol. 26, Issue 9, pp.2268-2280, 2014