International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 17 Issue 2 – SEPTEMBER 2015.

ENHANCMENT OF SECURITY AND PRIVACY PRESERVATION IN CLOUD DATABASE USING EFFICIENT SIGNATURE GENERATION

N.Santhini[#1], C.Theebendra[*2]

[#1]*M.phil, Research Scholar, Vivekananda Arts and Science College for women*
[*2]*Assistant professor, Department of Computer Science And Application, Vivekananda Arts and Science College for women*

***Abstract*--In cloud computing, the resources are shared between the cloud server and cloud user to achieve the communication such resources are hardware and software resources and it has high range of infrastructure requirements. The main concern is security and privacy issues are in cloud, hence the data leakage can available in cloud database. In previous methods, the encryption and decryption methods are used to hide the data from the hackers. However, this encryption method is not suitable for a large collection of cloud data. Therefore, we propose an efficient digital signature with mutual trust based control of access to detect and reduce the data leakage from the cloud database and also the privacy preservation can be increased. In this process, digital signature algorithm is used to verify the user's information and their authentication to the cloud server with the mutual trust based access control. The interaction can be occurred between the cloud server and user using the attributes and signature based. In our evaluation, the privacy preservation will be increased in cloud data storage.**

Keywords: Cloud Computing, Signature Generation Algorithm, Privacy Preservation, Access control.

I. INTRODUCTION

With the rapid growth of information within organizations, ranging from hundreds of gigabytes of satellite images to terabytes of commercial transaction data, the demands for processing such data are on the rise. Meeting such demands requires an enormous amount of low-cost computing resources, which can only be supplied by today's commercial cloud-computing systems: as an example, Amazon Elastic Compute Cloud (EC2) can easily handle terabytes of data at a price as low as 0.015 dollar per hour. This newfound capability, however, cannot be fully exploited without addressing the privacy risks it brings in: on one hand, organizational data contains sensitive information (e.g., financial data, health records, etc.) and therefore cannot be shared with the cloud provider without proper protection; on the other hand, today's commercial clouds do not offer high security assurance, a concern that has been significantly aggravated by the recent incidents of Amazon outages [1] and the Sony PlayStation network data breach [10], and tend to avoid any liability [3]. As a result, attempts to outsource the computations involving sensitive data are often discouraged. A natural solution to this problem is cryptographic techniques for secure computation outsourcing, which has been studied for a decade [8]. However, existing approaches are still not up to the challenge posed by data-intensive computing. For example, homomorphism encryption [9] was found to be prohibitively expensive for a large-scale computation [5]. As another example, the secret-sharing techniques underlying most outsourcing proposals can lead to intensive data exchanges between the share holders on different clouds during a computation involving an enormous amount of data, and are therefore hard to scale.

II. PROBLEM BACKGROUND

With a rapid development and acceptability of *computer vision based systems* in ones daily life, securing of the visual data has become imperative. **Security issues** in computer vision primarily originates from the *storage*, *distribution* and *processing* of the personal data, whereas **privacy concerns** with *tracking down* of the user's activity. The ideal solution to overcoming all privacy and security concerns is to apply strong cryptographic encryptions, thus destroying any pattern that would be present in that data. Pattern recognition, which is inherent to computer vision algorithms, however exploits the strong structure (pattern) present in the data. It seems that there exists a contradiction in the objectives of these two disciplines. Applying a strong encryption to this would destroy the structure, thus making any pattern recognition task on the encrypted data difficult. In order to overcome this limitation, solutions have been proposed that make a compromise

between privacy and accuracy. Transformation functions are applied to the data, such that they retain the pattern, while providing partial privacy The current methods of securing an online protocol is to apply a cryptographic layer on top of an existing processing module, thus securing the data against unauthorized third party access. However, this is often not enough to ensure the complete security of the user's privileged information. In the world of Internet, a new service sector has emerged, where a service provider gives the user with access to a server running a particular vision algorithm. In some scenarios, the client may be reluctant to reveal the content of the image to the processing server, yet would like to fully utilize the service, while at the same time the service provider would like to protect his own interests, i.e. the algorithm from being made public.

III. METHOD

Our Security Goal we aim to strengthen the security and privacy of the visual algorithms without making a compromise on the efficiency and efficacy of the solutions. The three primary issues in designing the privacy preserving protocols are i) security and privacy, ii) efficacy, and iii) efficiency. Hence, we analyze the secure algorithms for the security, correctness and complexity.

• Correctness is measured by comparing the proposed protocol to the ideal protocol where the parties transfer their data to a trusted third party that performs the computations. If the secure protocol is identical to the ideal protocol then the protocol is declared correct.

• In security one needs to show what can and cannot be learned from the data exchange between the parties. One often assumes that the parties are honest but curious, meaning that they will follow the agreed upon protocol but will try to learn as much as possible from the data flow between the two parties.

• In complexity, one shows the computational and communication complexity of the secure algorithm. For practical applications, the overheads of the proposed solution should be minimal as compared to the ideal solution.

We use the semi-honest adversary model that is the parties' follow the protocol but they want to reveal the other party's privacy. Our goal is to design protocols for preserving the party's privacy against such adversaries during the execution of the protocol. Each party learns nothing about the others data, except the output results. Both privacy and correctness are needed to be preserved. Forces against the secularism and human rights in not only in India and elsewhere.

IV. ALGORITHM FOR SCHEDULING

Step1: Read Input Job

Step2: Identify set of data objects necessary to execute the job.

Step3: compute similarity measure of data objects with semantic concepts.

Step4: Identify the semantic concept with respect to similarity measure.

Step5: retrieve the location of datasets from the indexed results.

Step6: return the results.

At the end of the scheduling process the application will be returned with the location of the cloud where the application has to be executed. The query processor will post the process to the returned location and will wait for the result and return the result to the application.

V. RESULTS AND DISCUSSION

The final results shows that our proposed scheduling algorithm reduces the overall execution time of the application by reducing the scheduling time and execution time. Our indexing scheme reduces the scheduling time.

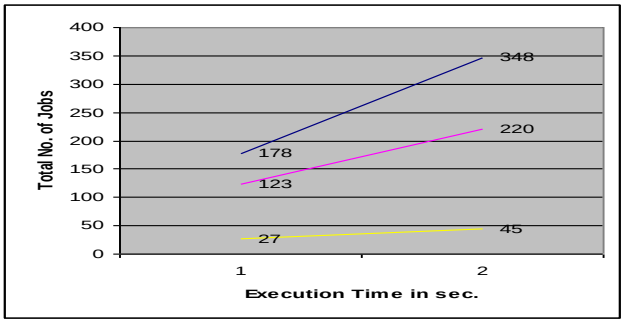

Fig: shows the analysis of different no. of process and time taken with different algorithm.

Blue line: Histogram based load balancing algorithm

Pink: Scp based scheduling

Yellow: Our algorithm.

VI. CONCLUSION

In accordance with various data and computation intensive applications on cloud, intermediate data set management is becoming an important research area. Privacy preserving for intermediate data sets is one of important yet challenging research issues, and needs intensive investigation. With the contributions of this

paper, we are planning to further investigate privacy aware efficient scheduling of intermediate data sets in cloud by taking privacy preserving as a metric together with other metrics such as storage and computation. As future work, firstly plan to improve the privacy preservation techniques to preserve more personalized details in application level. Secondly, we would like to propose a novel model for the security and privacy issues, which helps to achieve a confidential between provider and customer. Real cloud environment experiments for the proposed privacy preservation techniques are also expected in the near future

REFERENCE

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010.

[2] R. Buyya, C.S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud Computing and Emerging It Platforms: Vision, Hype, and Reality for Delivering Computing as the Fifth Utility," Future Generation Computer Systems, vol. 25, no. 6, pp. 599-616, 2009.

[3] L. Wang, J. Zhan, W. Shi, and Y. Liang, "In Cloud, Can Scientific Communities Benefit from the Economies of Scale?," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 2, pp. 296-303, Feb. 2012.

[4] H. Takabi, J.B.D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol. 8, no. 6, pp. 24-31, Nov./Dec. 2010.

[5] D. Zissis and D. Lekkas, "Addressing Cloud Computing Security Issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583-592, 2011.

[6] D. Yuan, Y. Yang, X. Liu, and J. Chen, "On-Demand Minimum Cost Benchmarking for Intermediate Data Set Storage in Scientific Cloud Workflow Systems," J. Parallel Distributed Computing, vol. 71, no. 2, pp. 316-332, 2011.

[7] S.Y. Ko, I. Hoque, B. Cho, and I. Gupta, "Making Cloud Intermediate Data Fault-Tolerant," Proc. First ACM Symp. Cloud Computing (SoCC '10), pp. 181-192, 2010.

[8] H. Lin and W. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 995-1003, June 2012.

[9] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data," Proc. IEEE INFOCOM '11, pp. 829-837, 2011.

[10] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS '11), pp. 383-392, 2011.