Load Balancing with Optimal Cost Scheduling Algorithm

Lovepreet
M.Tech Research Scholar
CEC Landran, Punjab, India

Sahil Vashisht
Assistant Professor
CEC Landran, Punjab, India

Abstract— **A cloud computing environment is proper load balancing technique that is required to implement a process and handle the resources. The distributed environment makes difficult to achieve resources have different configuration and capacity. The mapping of tasks to resources is done by load balancers, based on some particular objectives. Load balancers utilize a task that takes into version the necessary objectives to optimize a particular outcome. The tasks completion time and resource utilization are the most commonly used objectives of load balancing. It uses a precise loom to map the tasks to appropriate cloud resources in order to suit user requirements. Though, the maximum strategies are static in nature. A good schedule is produced which gives the existing status of cloud resources and do not report changes in resource availability. While current state of the system is considered by dynamic load balancers. It is reconciling nature and able to generate resourceful schedules. Thus, the overall performance of the system is improved. In this paper we have proposed to design new modal for key sharing and key management in fully Homomorphism Encryption scheme. Our aim is to understand the existing processor scheduling techniques and develop an optimized load balancing algorithm which gives maximum benefit to the cloud service provider.**

Index Terms—**Cloud, Load Balancer, Scheduling, Virtual Machines**

I. INTRODUCTION

Cloud computing is state that gives proper and on demand network access to a shared pool of computing resources like servers, networks, applications, storage and services that can be rapidly released with minimum management efficient way. Cloud is a centralized database where many clients /organizations store their data and possibly modify data and retrieve data [7]. CSP (Cloud Service Provider) provides services on cloud on pay per user base to user. Means here Client has to pay only for services he is with or being served. Cloud computing is a model for delivering services through which resources are retrieved from a centralized pool of resource. The cloud management software has to manage the resources at large scale. The key challenge is providing performance isolation and making efficient use of underlying hardware.

The basic approach involves the user accessing a resource when it is idle on a random basis. Cloud has become an alternative means of internet for most of us. Cloud represents ubiquitous computing. The two main entities involved in cloud computing are the cloud user and the cloud service provider. Sometimes a cloud broker may also exist. Any resources required by the user are delivered by the cloud service provider. The main aim of cloud provider is to maximize his revenue and at the same time, optimize the usage of the datacenter. The data center consists of processors, RAM, storage resources network resource, computing resource. The user gets the Quality of Service from the provider on the pay as- you-use basis. This can be achieved by optimal data center utilization and proper load balancing. Cloud computing is a technique which provides a huge range of applications under unlike kind of topologies and each topology derive new specialization. Yet cloud service provider like Drop box could unintentionally permit anyone to access any user's account devoid of user's knowledge. This would potentially lead to enormous data breaches which are away from user's control [4].

To fortify the security for cloud computing most organizations adopt standard enterprise security solutions like firewall, IPS and anti-virus. As users can now admittance cloud services from any place around the world, some organizations may employ stronger user verifications and access control solution as a defense against identity frauds. Unfortunately, these solutions do not really guard the user's information in the cloud. In this study our aim is to understand the existing processor scheduling techniques and develop an optimized load balancing algorithm which gives maximum benefit to the cloud service provider

II. LITERATURE SURVEY

Bhavna Makhija , VinitKumar Gupta, 2013, discuss the method of data security and privacy, in which they found that be short of underneath self-motivated data operations, few

were short of ensuring data integrity, elevated resource and totaling cost. They also described all accessible methods for cloud data security and techniques designed for ensuring data verification using TPA (Third Party Auditor). TPA is an inspector kind. It has two categories: private audit ability and public audit ability. Although private audit ability can attain superior scheme efficiency, public audit ability allow anyone, not only the client to defy the cloud server for the accuracy of storage space while keeping no personal information.

Dawn Song analyzed that its structural design noticeably decreases the per-application development effort required to offer data protection as still allowing fast development and maintenance [2].There are two technique FDE(fully disk encryption) and FHE (fully homomorphic encryption) are discussed .They compared both techniques based on key management ,sharing ,ease of development ,maintenance, accumulation and performance .The DPaaS loom moved key management and admittance control to a middle tier the computing stage to balance rapid development and trouble-free maintenance with user-side verifiability. Although FDE offers outstanding performance and effortlessness of development, it does less to protect privacy at the required granularity. FHE on the other hand, pushes the privacy packet in the other direction by removing data visibility wholly from both the server and application developer.

DeyanChen, HongZhao,2012, gave an examination on data security and confidentiality protection issues linked with cloud computing transversely all stages of data life cycle [3].The paper explained about prospect research work about data protection and confidentiality defense issues in cloud.

Deepanchakaravarthi Purushothaman and Dr.Sunitha Abbur described how to prevent Data access from unauthorized access so they proposed a distributed method that offers security of the data in cloud .This can be done by the use of homomorphism coupon with dispersed confirmation of removal of coded data [4].The Proposed technique perfectly stores the data and identifies at the cloud server and also execute some of the tasks such as data deleting, inserting and data updating . In this paper procedure to shun conspiracy attacks of server alteration by unauthorized access is also given. It explores various data encryption scheme like homophormic encryption, searchable and structured encryption, Identity based encryption, signature based encryption etc [5].

Sanjoli Singla and Jasmeet Singh projected design that helps to encode and decode the file at the client region which provides security to data and also while transferring the data [6] has been projected. In this research paper they combined Rijndael Encryption Algorithm with EAP-CHAP. From the customer view cloud computing security concerns in particular privacy protection and data security issues continue the primary inhibitor for acceptance of cloud computing services. So in this they looked on client side security. It is also planned that encoding must be done by the user to recommend better security Algorithm.

Mark D. Ryan , 2013 used techniques to protect data from a cloud infrastructure provider. They describe few issues with using fully homomorphic encryption in cloud computing applications. They anticipated a technique with which a browser key translation is allowed by software-as-a-service (SAAS) application to run with confidentiality from the service provider. They discover how trusted hardware can be used to defend cloud-based data.

III. RESEARCH OBJECTIVES

The following objectives of present work are as follows:

1. To analyze FHE and FDE encoding schemes for data protection in cloud computing
2. To enhance FHE encoding scheme for key executive and key distribution
3. The enhancement will be based on Diffie-Helman , HMAC and OTP technique for cloud data security
4. To implement proposed and existing schemes and compare results in terms of efficiency and escape time.

IV. RESEACH METHODOLGY

This study is mainly focused on to develop modal for fully homomorphism disk encoding scheme. This scheme will offer consistent key storage space and key managing services. It will boost the consistency and security of the offered fully homomorphism encoding scheme. In this new modal, secure channel establishment algorithm is used for key managing and key distribution The secure channel establishment algorithms are Diffie- Helman and RSA. The Diffie- Helman algorithm is a large amount protected and consistent algorithm. In the Diffie-Hellman algorithm if two clients say, Master and Slave wishes to swap data. Prior to starting the communication, secure channel is recognized. Both parties select their own random number. On the basis of the selected random numbers, secure channel and shared key is established.

Diffie Hellman Algo: Master and Slave wants to communicate with each other. To start communication both parties need to establish secure channel. To establish secure channel, two random prime number p and n are selected, both devices are agreed on these two numbers. Selected p and n are the public numbers. Both parties, say device 1 become master and device 2 become slave, both master and slave select their private numbers a' and 'b' respectively. Master and slave use their public and private number and calculated their private keys [26].

Master computes:

$M= p^a \bmod n$

Slave computes:

$S= p^b \bmod n$

Now both master and slave exchange their private keys such as 'M' and 'S'. After getting 'M' and 'S', master and slave calculates the secret keys such as K1, K2.

From S, master computes:

$K1= S^a \bmod n$

From M, slave computes:

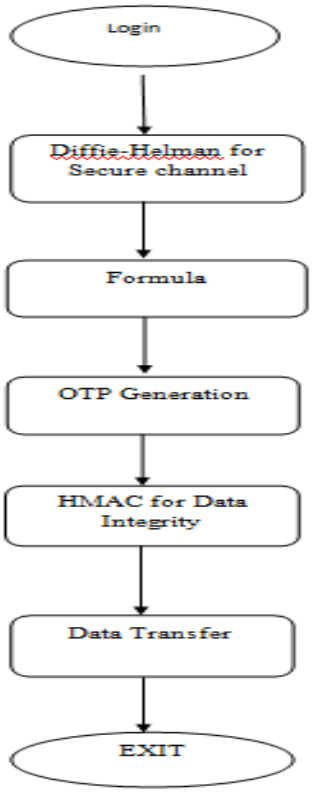
$K2= M^b \bmod n$

If both master and slave calculate same values of K1 and K2, then secure channel is established between them. The combination of K1 and K2 becomes the shared symmetric key between master and slave.

To encrypt the messages, they used the public key or shared key (K) of both parties. For decryption of messages private key of both parties which is randomly chosen by the users i.e. 'a' and 'b' are used.

The below given flow chart explains the proposed approach of further research. It describes the process. Firstly we do the

login procedure. As we started with the login, the channel gets secured with the Diffie- Helman algorithm. With the help of formulation of Diffie- Helman algorithm, OTP generation occurs. Further HMAC is responsible for the data integration. After the data integration, data is ready to be transferred securely through the particular channel.



V. CONCLUSION

Resource Scheduling is one of the mainly significant tasks in cloud computing environment. The new proposal will provide consistent key storage and key managing services. This will enhance the reliability and security of the existing fully homomorphism encryption scheme. In this new modal, secure channel establishment algorithm will be used for key managing and key distribution. The optimal cost scheduling algorithm which helps us to reduce the cost and the processing power. Cloud resources that have been used are minimal. The scheduling can be optimized and overall performance will be done using improved algorithm.

REFERENCES

[1] Bhavna Makhija,VinitKumar Gupta "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, 2013
[2] Dawn Song, Elaine Shi "Cloud Data Protection for the Masses" IEEE Computer Society, 2012
[3] Deyan Chen, Hong Zhao " Data Security and Privacy Protection Issues in Cloud Computing" International Conference on Computer Science and Electronics Engineering,2012
[4] Deepanchakaravarthi Purushothaman and Dr.Sunitha Abburu "An Approach for Data Storage Security in Cloud Computing" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1., 2012
[5] Simarjeet Kaur " Cryptography and Encryption In Cloud Computing" VSRD-IJCSIT, Vol. 2 (3), 2012, 242-249, 2012
[6] Sanjoli Singla, Jasmeet Singh "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7, July 2013
[7] Mark D. Ryan , "Cloud Computing for Enterprise Architectures: Concepts, Principles and Approaches", 2013
[8] Zvika Brakerski ,Vinod Vaikuntanathan "Effcient Fully Homomorphic Encryption "LWE, 2010
[9] Sigrun Goluch"The development of homomorphic cryptography" Vienna University of Technology, 2009
[10] Defence Signals Directorat "Cloud Computing Security Considerations" Cyber Security Operations Centre, 2011
[11] Ponemon Institute "Encryption in the Cloud Thales e-Security, 2009
[12] Anthony T. Velte Toby J. Velte, Ph.D. Robert Elsenpeter ,2010 "Cloud Computing: A Practical Approach" 2011
[13] Zhang, Z., Plantard, T., & Susilo, W. (2012). Reaction attack on outsourced computing with fully homomorphic encryption schemes. In Information Security and Cryptology-ICISC 2011 (pp. 419-436). Springer Berlin Heidelberg
[14] Craig Gentry, 2009,"full homomorphic encryption scheme"
[15] Zvika Brakerski, Vinod Vaikuntanathan, 2009 "Efficient Fully Homomorphic Encryption "LWE
[16] Sigrun Goluch 2009 "The development of homomorphic cryptography" Vienna University of Technology
[17] Sanjoli Singla,Jasmeet Singh (july 2013) "Cloud Data Security using Authentication and Encryption Technique" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 7
[18] John Harauz ,Lori M. Kaufman,Bruce Potter," Data Security in the World of Cloud Computing " IEEE Security and Privacy July 2009. pp. 61-64
[19] van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V (2010) Fully homomorphic encryption over the integers. In Gilbert, H., ed.: EUROCRYPT. Volume 6110 of Lecture Notes in Computer Science., Springer
[20] Hamlen, K., Kantarcioglu, M., Khan, L., & Thuraisingham, B. (2010). Security issues for cloud computing. International Journal of Information Security and Privacy (IJISP), 4(2), 36-48.

