Exploiting Task Elasticity & Performance Guarantee for Cloud Data Sharing System

Mr. Akarsh Kapasi[1] Ganesh Devidas Solanke[2] Venkatesh Santoshdas Vaishnav[3] Hanumant Rajaram Salve[4]

[1,2,3,4]Department of Information Technology

[1,2,3,4]D Y Patil College of Engineering, Akurdi, India

Abstract— Cloud computing is a strategy for conveying data innovation (IT) benefits in which assets are recovered from the Web through online instruments and applications, rather than an immediate association with a server. Instead of keeping documents on a restrictive hard drive or nearby stockpiling gadget, cloud-based capacity makes it conceivable to spare them to a remote database. For whatever time allotment that an electronic device approaches the web, it approaches the data and the item ventures to run it. It's called cloud computing in light of the fact that the data stored in” the cloud” and does not require a client to be in a particular place to access it. This sort of system empowers agents to work remotely. Organizations giving cloud administrations empowers clients to store records and applications on remote servers, and after that entrance every one of the information by means of the web. Information and Data security and access control is a testing research work in cloud computing. Cloud benefit clients transfer their private and secret information over the cloud. Security must be given to such outsourced information, with the goal that client is not stressed while transferring their classified information.

Key words: LDSS, Byte Rotational Algorithm (BRA), UCI

I. Introduction

For proposing an online asset, the board outline work that expands benefit proportion while limiting vitality costs by misusing the dispersed undertaking versatility and value heterogeneity. This is finished by lessening the term amid which servers should be left ON and boosting the money related incomes when the charging cost for a portion of the inelastic errands relies upon how quick these undertakings complete, while meeting all asset prerequisites. The power supply and the center speed are expanded when there are more assignments in server, to such an extent that errands can be handled quicker and the normal undertaking reaction time is reduced. It is conceivable to structure a multicore server processor with remaining burden subordinate unique power the board, to such an extent that its normal assignment reaction time is shorter than a multicore server processor of steady speed (i.e., without outstanding task at hand subordinate powerful power the executives). Byte Rotational Algorithm (BRA) gives greater security and sets aside littlest measure of time for exchange record. This calculation can apply on various sorts of documents like content, picture, sound, video records.

Near investigations directed utilizing UCI storehouse information follows demonstrate the adequacy of our proposed structure as far as enhancing asset use, diminishing vitality costs, and expanding benefits proportion by figuring memory and transfer speed with expanding speed. The procedure versatility is misused on heterogeneous condition in a conveyed framework. Versatility is how much a framework can adjust to remaining burden changes by provisioning and de-provisioning assets in an autonomic way, with the end goal that at each point in time the accessible assets coordinate the present interest as nearly as would be prudent. Different methodologies are viewed as like sequential, parallel and half-breed approaches. As needs be, benefit proportion is determined. Process mining is taken as an undertaking to figure the benefit proportion. Assets that are considered are CPU, Bandwidth, Time and Temperature and Memory. Instruments used to figure the benefit proportion of CPU, Bandwidth, Time and Temperature and Memory is CPU-Z and HW-Monitor. The assignments included are free on one another. Benefit proportion is determined of variables i.se CPU, Bandwidth, Memory, Time and Temperature of frameworks with various processors.

II. Literature Survey

A. Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

A lightweight information sharing plot (LDSS) for portable distributed computing. It receives CP-ABE, an entrance control innovation utilized as a part of typical cloud condition, be that as it may, changes the structure of access control tree to make it reasonable for versatile cloud situations. LDSS moves a vast segment of the computational serious access control tree change in CP-ABE from cell phones to outer intermediary servers. Moreover, to lessen the client renouncement cost, it acquaints property depiction fields with execute apathetic disavowal, which is a prickly issue in pro-gram-based CP-ABE frameworks. The trial comes about demonstrate that LDSS can successfully lessen the overhead on the cell phone side when clients are sharing information in portable cloud situations.

B. Low Latency for File Encryption and Decryption Using BRA Algorithm in Network Security

Data security is significant deterrent in various zones like military, bank application, educational organization. Document is forward starting with one area then onto the next area in organize. Numerous programmers are unlawfully get to the data. To give answer for this issue many creators has presented diverse calculations and strategies. The distinctive calculations like DES, triple DES and AES accomplish greater security however it sets aside more opportunity for encryption and decoding records. This algorithm gives greater security and takes littlest measure of time for record encryption and decoding. This encryption can apply on various sorts of records like content, picture, sound, video records. In the Byte Rotation Encryption Algorithm include two procedures. One is irregular key era procedure is utilized. What's more, second is parallel encryption and decoding is process utilizing multithreading procedure.

C. *Analysis of Multi-Threading Time Metric on Single and Multi-Core CPUs with Matrix Multiplication*

With the landing of multi-center CPUs, to accelerate execution of frame-works utilizing parallelism is prompting new approaches. Prior techniques to actualize parallelism in applications were constrained to either utilization of excess equipment assets or direction level parallelism (ILP). This requested the need of part the undertaking or process into little sections that can keep running in parallel in the errand's unique circumstance, and strings have been presented. It is normal that the quantity of centers per processor would duplicate with increment in silicon do- main on chip. Keeping in mind the end goal to achieve most extreme center usage of equipment, programming needs to flourish. Multi-threading is prevalent approach to enhance application execution speeds through parallelism. As each string has its possess autonomous asset for assignment execution, various procedures can be executed parallel by expanding number of strings. Parallelism is the running of strings in the meantime on centers of a similar CPU. Multi-threading is famous approach to enhance application execution speeds through parallelism. As each string has its claim free asset for assignment execution, various procedures can be executed parallel by expanding number of strings. Parallelism is the running of strings in the meantime on centers of a similar CPU.

III. FUTURE SCOPE

We will develop a mobile application for mobile computing. We can develop the multi-cloud system. We can apply better 3D encryption algorithm for better security and efficiency.

A. *Proposed System*

To overcome from the security and data privacy issues in conventional cloud computing. To share sensitive data among users and provide security to data on cloud and to maintain the integrity of the data in cloud storage. It abuses the procedure flexibility on heterogeneous condition proposed by the asset the executive’s system that augments benefit while computing Memory, Time, Temperature and Bandwidth by taking procedure mining as assignment. To build a framework similar to Remote Storage System where User Information can efficiently Store in Decentralized Network Using Chunking Mechanism. Faster Upload/Download features can be achieved through Our Approach.

To share a data between different users securely and to maintain the integrity of the data with the help of –

1) Chunking Algorithm
2) Byte Rotation Encryption Algorithm

B. *System Architecture*

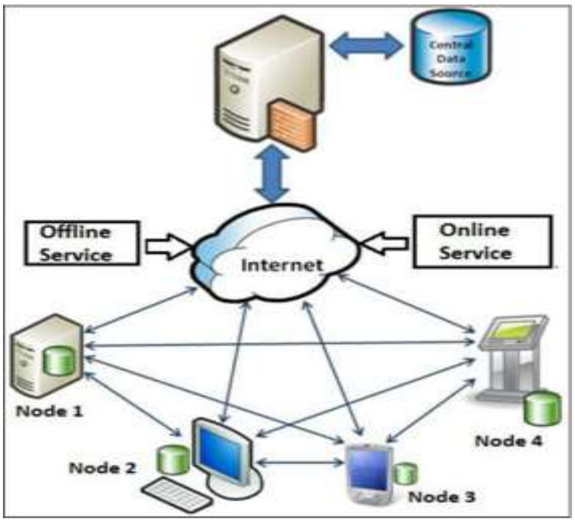

Fig. 1: System Architecture of Proposed System

C. *System Specification*

1) *Hardware Requirements*

- Processor: Pentium IV
- CPU Speed: 2 GHz and above.
- RAM: 512 MB and Above
- OS: Ubuntu 14.04 and Above
- Browser: Chrome/Mozilla.

2) *Software Requirements*

- Operating System: Linux
- IDE: Eclipse (juno) / Netbeans 8.2
- Programming Language: JAVA,JSP
- Java Version: JDK 1.7 or Above
- Database: MySQL 5.5
- Web Technology: JSP, Servlet, HTML, CSS, Javascript
- Web Server: Apache Tomcat 6.0

IV. PROPOSED SYSTEM

File Sharing is the one of the most widely used concept in today’s digital world. Associated to the File Sharing are also the Peer-to-Peer (p2p) applications. Among all the p2p applications, file sharing is the most popular one. The traditional client/server file sharing lacks the few key benefits when compared to the Peer-to-Peer file sharing, one of which is Scalability. On facing the increase in the number of clients the performance of the traditional client/server file sharing decreases rapidly. In case of well-built Peer-to-Peer File Sharing System the condition is well handled, since the load is distributed to all participating peers.

BitTorrent is the main application for the Peer-to-Peer File Sharing. BitTorrent is a popular peer-to-peer _le-sharing protocol that has been shown to scale well to very large peer populations. With BitTorrent, content (e.g., a set of _les) is split into many small pieces, each of which may be downloaded from different peers. The substance and the arrangement of friends dispersing it is typically called a downpour. A companion that just transfers content is known as a seed (Peers that have the entire record), while a friend that transfers and downloads in the meantime is known as a leecher. The associated set of companions taking an interest in the piece trades of a deluge is alluded to as a swarm. In a

BitTorrent network, a single file is shared by many users. The main feature of BitTorrent is that the shared file is divided into many pieces (the default size of a piece is 256KB), so a peer could start to serve others even if it does not have a complete file. While other peers with partial or none of the file are called downloaders, when a peer first joins the network, it connects to a central server called tracker to get a list of peers. The new peer then connects to those peers to request for pieces and those peers become the neighbors of the new peer. Once the new peer obtains at least one pieces, it can start to contribute to the network uploading to others. The peer then exchanges pieces with its neighbors until it obtains all pieces and becomes a seed. The distributed property of file sharing process makes the BitTorrent scalable.

A. Algorithms

1) Attribute Based Encryption Algorithm:

1) Step 1: Start
2) Step 2: Generating the symmetric key for the register users.
3) Step 3: A set of user attributes is supplied to the input of the private key generation, and the output of the algorithm turns user's private key.
4) Step 4: The input is fed to the encryption function which it is necessary to encrypt, a set of attributes, decryption of data will be done by owner, and randomly selected number, and the output will be obtained encrypted data.
5) Step 5: A set of user attributes AU and the encrypted data are supplied to the input of the decryption function, and the output will be obtained decrypted message.
6) Step 6: Safe data retrieval.
7) Step 7: End

2) Byte Rotation Algorithm

1) Step 1: Start
2) Step 2: The Data is partitioned into fixed length of blocks. These blocks are represented by matrix Mp.
3) Step 3: The numerical values is assigned to the data in sequence.
4) Step 4: The value of Key matrix is randomly selected from the given range.
5) Step 5: Calculate the Transpose matrix of data block matrix Mp which is denoted by Mt.
6) Step 6: Calculate the encrypted key matrix Kc .
7) Step 7: Add both matrix Mt and Kc. The resultant matrix is denoted by Cpk.
8) Step 8: Rotate the first 3 row horizontally of Cpk matrix. The resultant matrix will be matrix Chr.
9) Step 9: Rotate the first 3 column of Chr matrix. The resultant matrix is denoted by Cvr.
10) Step 10: Replace the numerical values of Cvr matrix by the corresponding blocks.

3) Mathematical Model

1) Input: Collection of different types of dataset e.g.- docx , pdf, xlsx, etc.
2) Output: Encode/Decode information as per request
3) Methodology:
4) Attribute Based Encryption Algorithm
5) Byte Rotation Encryption Algorithm

4) Function

1) Authentication of users
2) Encoding data
3) Decoding data
4) Serial operation
5) Parallel operation

5) System Description

Let S be the Whole system which consists:

S= {m, ƛ, s, x, r, P}

1) m= Total cores available on multicore system 'S'
2) ƛ= arrival time of each task which want to execute on multicore system.
3) s= Execution speed of 'm' cores on multicore system 'S' Now,

Total task execution time(x) = r/s

Here,

– x=Execution time
– s=Execution speed
– r=Total speed rate of task

Acknowledgment

We have taken efforts in this project. Be that as it may, it would not have been conceivable without the caring help and help of numerous people and associations. We might want to stretch out my genuine because of every one of them. We are highly indebted to Mr. Akarsh Kapasi for his guidance and constant supervision as well as for providing necessary information regarding the project & also for his support in completing the project. We would like to express my gratitude towards my parents & my Head of I.T. Department for their kind co-operation and encouragement which helped us in completion of this project. Furthermore, we would also like to acknowledge with much appreciation the crucial role of the staff of DYPCOE Akurdi, who gave the permission to use all required equipment and the necessary materials to complete my project. We also are deeply grateful to the Principal of DYPCOE, Dr. Vijay Wadhai and my parents for their financial and logistical support and for providing necessary guidance concerning project’s implementation.

References

[1] Mehar Dabbagh, Bechir Hamdaoui, Mohsen Guizani, Ammar Rayes, Exploiting pro_t ratio by process elasticity on heterogeneous environment" VOL. 27, NO.6, JUNE 2015.

[2] Maitri, Dattatray S. Waghole, Vivek S. Deshpande, IEEE Senior Member, \Low latency for _le encryption and decryptionusing BRA algorithm in network security", 2015 International Conference on Pervasive computing.

[3] BingChun Chang, \A Running Time Improvement for Two Thresholds Two Divisors Algorithm", December 2009.

[4] M. NoroozOliaee, B. Hamdaoui, M. Guizani, \Online multiresource scheduling for minimum task completion time in cloud servers," in Computer Communications Workshops, 2014 IEEE Conference.

[5] M. NoroozOliaee, B. Hamdaoui, M. Guizani, and M. Ben Ghorbel, \Online multiresource scheduling for minimum task completion time in cloud servers," in Computer Communications Workshops, 2014 IEEE Conference on. IEEE, 2014, pp. 375{379}.