INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

COMPARATIVE STUDY AND EXPERIMENTAL ANALYSIS OF STORAGE AND SECURITY OVER CLOUD

[1]Priyanka Gidwani, [2]Prof. Sreeja Nair

[1]Scholar, Computer Science and Engineering, Oriental Institute of Science and technology Bhopal, India
[2]Professor, Computer Science and Engineering, Oriental Institute of Science and technology Bhopal, India
Email: Priyankagidwani1@gmail.com, sreejanair@oriental.ac.in

Abstract: - Cloud computing has shaped the theoretical and infrastructural basis for tomorrow's computing. The global computing infrastructure is quickly moving towards cloud based structural design. While it is significant to take advantages of cloud based computing by means of deploying it in diversified sectors, the safety aspects in a cloud based computing environment vestiges at the core of interest. Cloud computing platforms offer easy accessibility to a company's superior computing and storage infrastructure through internet services. This model works on pay on demand service, if anyone needs to use the resources than he use to purchase that resources for specific amount of your time to finish the task. Thanks to this technology we are able to get several profits in terms of value, load leveling, time, speed, energy &so on. Value reduction is a very important issue and security of information ought to even be maintained in cloud computing. the present methodologies that job on minimizing the value of information storage is Pretty sensible verification-PGV, Multiple key Cryptography(MKC), SecCloud that could be a initial protocol bridging secure storage and secure computation auditing in cloud and achieving privacy cheating discouragement. These technologies focuses on the value reduction solely however during this paper security of information keep is additionally maintained by using compression and decompression technique LZW that is safer than those used antecedently. We tend to found that LZW is way higher than alternative techniques.

Keywords—MKC, LZW,compression, decompression

I. INTRODUCTION

Cloud computing is presently rising as a mechanism for prime level computation, likewise as serving as a storage system for resources. It works supported Pay on Demand model. This model suggests that, within which amount user needed the resources for a selected time to complete a task, user ought to pay some cash just for that abundant of your time. Owing to this technology several edges square measure applicable to induce the higher profit within the market. Profit in terms of your time, cost, load reconciliation, storage and then on. Cloud storage usually refers to a hosted object storage service, however the term has broadened to incorporate different styles of information storage that square measure currently obtainable as a service, like block storage. Cloud storage could be a service model within which information is maintained, managed and insured remotely and created obtainable to users over a network.

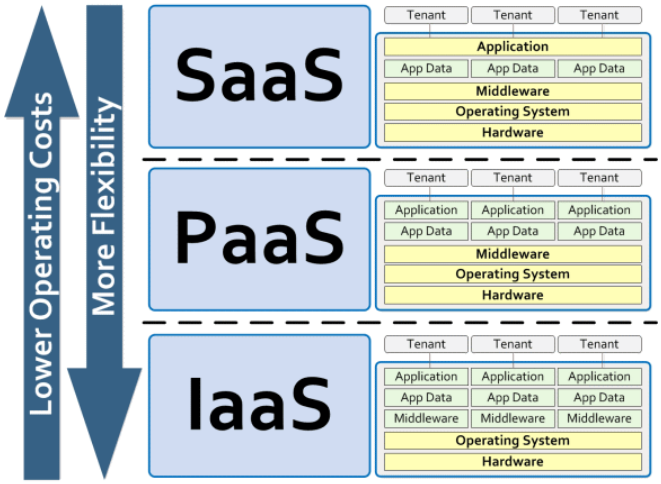


Fig 1. Cloud Service Model

During this analysis we have a tendency to provide stress on doing cloud storage analysis with relevance information security and inexperienced cloud as a result of these 2 attributes square measure more practical for value decrease and providing secure cloud. Additionally, only a few researchers have self-addressed these 2 attributes along. Through our methodology we have a tendency to square measure able to scale back a big quantity of value by providing a considerable security. Furthermore our methodology will be able to offer information integrity with the assistance of LZW algorithm. The projected methodology could be a new thanks to offer a value effective and secure cloud service. During this security technique code is additionally used for secret writing the info. Lempel-Ziv-Welch proposed a variant of LZ78 algorithms, in which compressor never outputs a character, it always outputs a code. To do this, a major change in LZW is to preload the dictionary with all possible symbols that can occur. LZW compression replaces string of characters with codes.

Recent developments in the field of could compute have immensely changed the way of computing as well as the concept of computing resources. In a cloud based computing
infrastructure, the resources are normally in someone else's premise or network and accessed remotely by the cloud users (Petre, 2012; Ogigau-Neamtiu, 2012; Singh & jangwal, 2012). Processing is done remotely implying the fact that the data and other elements from a person need to be transmitted to the cloud infrastructure or server for processing; and the output is returned upon completion of required processing. In some cases, it might be required or at least possible for a person to store data on remote cloud servers. These gives the following three sensitive states or scenarios that are of particular concern within the operational context of cloud computing:

• The transmission of personal sensitive data to the cloud server,
• The transmission of data from the cloud server to clients' computers and
• The storage of clients' personal data in cloud servers which are remote server not owned by the clients.

Dong Yuan in his paper build associate intermediate information dependency graph (IDG) from the info provenances in scientific workflows. With the IDG, deleted intermediate datasets may be regenerated, and in and of itself we have a tendency to develop a unique algorithmic program that may notice a minimum value storage strategy for the intermediate datasets in scientific cloud progress systems [1]. Lifei dynasty proposes a privacy cheating discouragement and secure computation auditing protocol, or SecCloud, that could be an initial protocol bridging secure storage and secure computation auditing in cloud and achieving privacy cheating discouragement by selected voucher signature, batch verification and probabilistic sampling techniques [2]. Mahomet Iftekhar Husain presents a storage implementing remote verification theme, PGV (Pretty smart Verification) as a bifacial information integrity checking mechanism for cloud storage. PGV depends on the

tendency toll- notable polynomial hash; we show that the polynomial hash demonstrably possesses the storage social control property [3]. This paper is projected by Nidhi Bansala during this the price is calculated of QoS-driven task planning algorithmic program and compare with ancient task planning algorithmic program in cloud computing setting. The experimental results supported cloudsim3.0 toolkit with Net Beans IDE8.0 shows that QoS-driven achieves smart performance in value parameter [4]. Maurizio Giacobbe in his paper the huge exploitation of ICT solutions is increasing the energy consumption of suppliers, so several researchers square measure presently investigation new energy management strategies [5].

II. PROBLEM IDENTIFICATION

1. Security & privacy

This group includes managerial and technical issues related to keeping cloud services at an satisfactory level of information security and data solitude. This includes ensuring safety and privacy of susceptible data held by banks, medical and examines amenities. Security and privacy issues become even more somber when governmental organizations use the cloud. In spite of the recognized need for Service Level Agreements between Cloud service providers and users, standards for security have not yet been recognized and more research in this area would be helpful. Security and privacy of data spans issues such as authentication, encryption, and discovery of malware, side channel attacks and other kinds of attacks—both internal and external to an enterprise.

2. Infrastructure

This category entails matters pertaining to the hardware layer used as a base for cloud services as well as the thin layer of software used to function this hardware. The main problem that dominates this category is performance including the topics like SaaS placement issues, server allocation optimization, load balancing and many others. Other challenges are related to networking such as traffic management, ever-present connectivity, network speed and cost, and network reliability. Another group of challenges be relevant to resource management including dynamic resource provisioning, scaling, and allocation; as well as resource stranding and disintegration.

3. Data management.

As cloud computing is enabling more data-intensive applications at the extreme scale, the demand is increasing for effective data management systems. One main topic in this category is data storage and all the issues that come with it such as data federation (i.e. storage across different providers), data segmentation and recovery, data resiliency, data fragmentation and duplication, and data backup. Other issues include data retrieval and processing, data provenance, data anonymization, and data placement (across different data centers).

4. Interoperability.

Most research on issues and challenges with cloud computing recognize interoperability as a major adoption barrier because of the risk of a vendor lock-in. Amongst the many problems being discussed are: the lack of standard interfaces and open APIs, and the lack of open standards for VM formats and service deployment interfaces. These issues result in integration difficulties between services obtained from different cloud providers as well as between cloud resources and internal legacy systems.

5. Legal issues.

The notion of using cloud resources as a utility has brought about a number of legal issues. The most discussed issue in the literature we surveyed is related to data placement. Laws and regulations vary widely across different regions and jurisdictions as to where and how data should be stored, processed, and used. For example, the European Union requires that all personal data be physically stored within the jurisdictions of the European

Union. Also, compliance requirements might vary in regards to the disclosure of data in general and sensitive data in specific (e.g. financial data, health insurance records), in addition to variations in the regulations around transaction logging and taxation.

III. METHODOLOGIES

1 Task scheduling-

In this we have a tendency to alter 2 algorithms that square measure Traditional programming algorithmic program FCFS and Optimized programming algorithmic program QoS driven. The temporary descriptions for these programming ways square measure delineate here. First methodology that's FCFS (first come back initial serve).This programming algorithmic program is extremely common in methodology. It's a straightforward methodology to develop. It uses non pre-emptive methodology for programming within which all processes square measure mechanically placed within the queue and select process in keeping with user request.

Second methodology planned a programming algorithmic program supported QoS-driven in Cloud Computing with considering execution time, load equalization and latency. This algorithmic program supported user necessities, user rights, method expectation, method length and therefore the execution time to cipher the task priority.

Figure one shows the fundamental model for execution of programming algorithmic program victimization Cloudsim . In the cloud computing system initial of all cloudsim machine package is initialized then datacenter then broker then virtual machines so cloudlets or tasks. Then it communicates with the virtual machines after it scheduling executes.
Finally show the results.

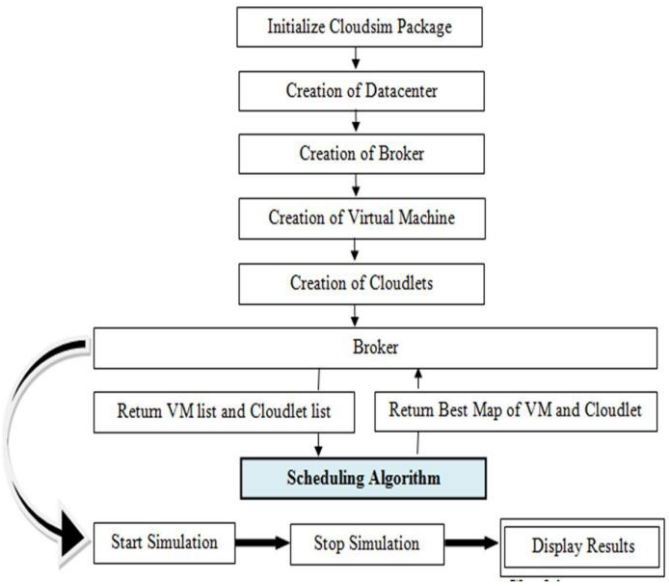


Fig 2 – Flowchart of the Methodology

2 Pretty Good Verification-

IT uses a polynomial recap a finite field to envision whether or not the storage supplier still has the info that client sent them. They generate one or additional keys arbitrarily, hash the info with the keys, and store the keys and hashes along. once time involves do verification, they send as single key to alternative remote finish, and elicit them to reason the keyed hash and send it back, comparison the result with what's keep. To reason a polynomial hash, a shopper has to choose system- wide parameters once and perform 3 steps whenever

exportation information block to an overseas storage. There square measure 2 necessary system wide parameters: the finite field size and also the block size (e.g., 64KB).Picking the correct values for these parameters involves concerns for performance and security. We tend to discuss these concerns any in our analysis. Once the shopper finishes choosing the system wide parameters, the shopper will reason a polynomial hash for every information block to be exported:

(i) choose a random variety (key) β from the sector,
(ii) divide the info block into equal-sized symbols, S0;…; Sk_1, wherever the scale is adequate to the sector size(e.g.,4B),
(iii)compute the polynomial hash Hc ¼Σk_1 i ¼ 0Siβi.This is resembling computing a facet and also the quantity of communication and wish to attenuate each at the same time whereas giving smart verification properties. The PGV state of affairs wherever a shopper verifies an overseas server (or multiple servers).

3 Multiple Key Cryptography-

We are usually famed with bilaterally symmetrical cryptography that is finished through single key secret writing and public key cryptography that is finished through 2 keys named non-public key and public keys. MKC could be a method wherever secret writing and cryptography is finished through multiple keys. Thus here multiple keys secret writing is employed to encode plaintext into cipher text. Here same multiple keys are accustomed convert cyphertext in reverse order to seek out the most plaintext throughout cryptography.

4 Elliptic Curve Cryptography-

Elliptic curve cryptography is Associate in Nursing approach to public key cryptography supported the pure mathematics structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was advised severally by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. For current cryptanalytic functions, Associate in Nursing elliptic curve may be a plane curve over a finite field (rather than the $64000 numbers) that consists of the points satisfying the equation along with a distinguished purpose at time, denoted ∞.This set beside the cluster operation of elliptic curves is Associate in Nursing mathematical group, with the purpose at time as identity operator. The structure of the cluster is inheritable from the divisor cluster of the underlying pure mathematics selection.

5. LZW Algorithm -

In 1980, Terry Welch invented LZW algorithm which became the popular technique for generalpurpose compression systems. It was used in programs such as PKZIP as well as in hardware devices. Lempel-Ziv-Welch proposed a variant of LZ78 algorithms, in which compressor never outputs a character, it always outputs a code. To do this, a major change in LZW is to preload the dictionary with all possible symbols that can occur.

LZW compression replaces string of characters with codes. LZW algorithmic rule may be a lossless information compression algorithmic rule that is predicated on dictionaries [1]. This LZW mechanical device maintains records with characters that are browse from a file to be compressed. every character is delineated by AN fact within the lexicon. During this paper, we tend to projected a improve theme for information compression.**LZW Compression:**

```
w = NIL;
While (read a character k )
    {
        if wk exists in the dictionary
                w = wk;
        else
                add wk to the dictionary;
                output the code for w;
        w = k;
    }
```

LZW Decompression:

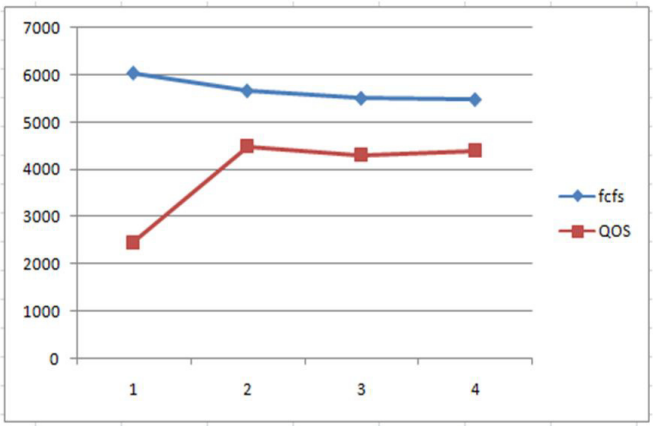
```
read a character k;
        output k;
        w = k;

  while ( read a character k )
 /* k could be a character or a code. */
  {
        entry = dictionary entry for k;
        output entry;
        add w + entry[0] to dictionary;
        w = entry;
   }
```

IV.RESULTS

The results of the previous scheme used are compared on the basis of their given statistics

1 Task scheduling-

In this paper analyses have been done between two algorithms that are FCFS and QoS



Tabulated representation of results is also mentioned here in Table

Fig 4 - Analysis of scheduling algorithms

Cloudlets	FCFS	QoS
50	5668.944	4481.248
70	5512.491	4298.72
100	5486.416	4398.984

Table 1 – Comparison of FCFS and QoS results

2 Pretty Good verification-

In this paper it shows the comparison between PGV & PDP on the basis of benchmark there comparison is represented through tables. Table 2 shows a benchmark summary on the experimental platform of cryptographic algorithms. Table 3 shows a benchmark summary of Galois field multiplication and encoding.

Table 2: Performance of different primitives

Field	Multiplication	Encoding (MB/s)
GF(2^16)	269	110
GF(2^32)	106	25

Table 3: Performance of multiplication and encoding

3. LZW Algorithm-

In this technique they have received 47.07% reduction rate on average within the range -0.76% to93.37%. So the reduction rate mostly depends on types of files stored in cloud. According to our statistics if 47.07% data size can be reduced then 47.07% space will be saved in cloud storage which also saves 47.07% total energy that is required for storage by ignoring computational overhead of these small files on a large cloud data center.

V. CONCLUSION

This approach would be able to reduce the space required to save data in cloud storage with security, so we can say that cost minimization is possible through less space used and less power consumption in cloud storage. In this approach we are using LZW algorithm for minimum cost with optimum storage to provide better security.

VI. REFERENCES:

[1] B.R. Kandukuri, V.R. Paturi and A. Rakshit "Cloud security issues. “Services Computing, 2009. SCC'09. IEEE International Conference on.IEEE, 2009.
[2] M. Islam and M. Habiba, "Agent based framework for providing security to data storage in cloud." In Computer and Information Technology (ICCIT), 2012 15th International Conference on, pp. 446-451. IEEE, 2012.
[3] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in: 14th European Symposium on Research in Computer Security (ESORICS’09), Saint Malo, France, September 21–23, 2009.
[4] S.S. Rawat, N. Sharma, A new way to save energy and cost – cloud com1152 putting, Intl J Emerg. Technol. Adv. Eng. 2 (2012) 83–89.
[5] A. Jain,M.Mishra, S. Peddoju, N. Jain, Energy efficient computing green cloud computing, in: Energy Efficient Technologies for Sustainability(ICEETS), 2013 International Conference on, 2013, pp. 978–982.
[6] W. Itani, A.I. Kayssi, A. Chehab, Privacy as a service: privacy-aware data storage and processing in cloud computing architectures, in: Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC 2009), Chengdu, China, December 12–14, 2009.