A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage

Gunda Sarath Kumar [1], D.Rammohanreddy[2]
[1]*Pursuing M.Tech (software engineering), Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*
[2]*Associate Professor,Newton's Institute of Engineering College, Alugurajupally, macherla, Guntur dist, AP, India*

***Abstract*- As an important application in cloud computing, cloud storage offers user scalable, flexible and high quality data storage and computation services. A growing number of data owners choose to outsource data files to the cloud. Because cloud storage servers are not fully trustworthy, data owners need dependable means to check the possession for their files outsourced to remote cloud servers. To address this crucial problem, some remote data possession checking (RDPC) protocols have been presented. But many existing schemes have vulnerabilities in efficiency or data dynamics. In this paper, we provide a new efficient RDPC protocol based on homomorphic hash function. The new scheme is provably secure against forgery attack, replace attack and replay attack based on a typical security model. To support data dynamics, an operation recordable (ORT) is introduced to track operations on file blocks. We further give a new optimized implementation for the ORT which makes the cost of accessing ORT nearly constant. Moreover, we make the comprehensive performance analysis which shows that our scheme has advantages in computation and communication costs. Prototype implementation and experiments exhibit that the scheme is feasible for real applications.**

I. INTRODUCTION

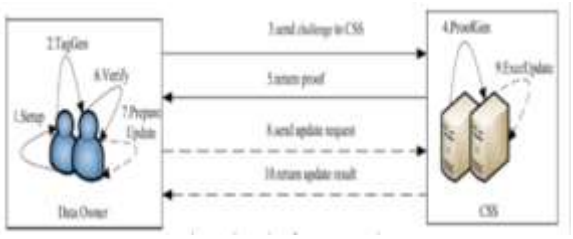
IN the previous couple of years, we have seen the colossal improvement of distributed computing, with to an ever increasing extent cloud administration suppliers hopping on the cloud fleeting trend. Alongside the steady development of huge scale open cloud suppliers like Amazon EC2[2], Windows Azure and Rack space , little scale cloud suppliers, for example, Ready- Space and Gorged have overwhelmingly risen. Notwithstanding the buildup about distributed computing, in any case, the genuine reception rate of distributed computing is still behind desire [9], particularly outside the United States. Unmistakably, to the whole cloud industry, it is pivotal to animate end clients' support in distributed computing. From a person cloud administration supplier's viewpoint, it is vital to keep its aggressiveness among associate cloud administration suppliers. As broke down in, the best way to distributed computing achievements to create sufficient evaluating strategies. In a framework as-an administration (IaaS) cloud, the cloud supplier powerfully fragments the physical machines, utilizing virtualization advances, to suit different virtual machine (VM) asks for from its clients. On a fundamental level, the clients just need to pay for the asset they really expended. By and by, the compensation as-you-use estimating .model is right away just ideological because of the high multifaceted[10] nature in observing and evaluating asset use, for example, system transfer speed, virtual CPU time, memory space, and so on. Therefore, true charging plans in IaaS cloud have turned out to be irrationally confused.

II.LITERATIRE SURVEY

Theoretical Background:
In project developed .net by using software requirements Database is SQL Server 2008 And Visual Studio, Frontend is used language ASP.

Domain Description:
Cloud Computing:
Distributed Cloud computing is a type of computation in which many calculations are carried out simultaneously, operating on the principle that large problems can often be divided into smaller

ones, which are then solved at the same time to achieve a common goal. Three significant characteristics of distributed systems are: concurrency of components, lack of a global clock, and independent failure of components. Examples of distributed systems vary from SOA-based systems to massively multiplayer online games to applications. A computer program that runs in a distributed system is called a distributed program, and distributed programming is the process of writing such programs.[2]There are many alternatives for the message passing mechanism, including pure HTTP, RPC-like connectors and message queues.



Existing System:

- The first RDPC was proposed by Deswarte et al. based on RSA hash function. The drawback of this scheme is that itneeds to access the entire file blocks for each challenge.
- In 2007,the provable data possession (PDP) model was presented byAttendees et al., which used the probabilistic prooftechnique for remote data integrity checking without accessingthe whole file. In addition, they supplied two concrete schemes(S-PDP, E-PDP) based on RSA.

DISADVANTAGES OF EXISTING SYSTEM:

- Did not Support Dynamic Operations.
- Heavy Computation Cost.
- Insecure against replay attack and deletion attack.
- These schemes are either insecure or not efficient enough.

PROPOSED SYSTEM:

- We present a novel efficient RDPC scheme with data dynamics. The basic scheme utilizes homomorphic hashfunction technique, in which the hash value of the sum for twoblocks is equal to the product for two hash values of thecorresponding blocks.

ADVANTAGES OF PROPOSED SYSTEM:

- Experiment results show that the new scheme has better performance and is practical for real applications.
- We show the advanced RDPC scheme supporting fully dynamic block operations based on ORT.
- Minimum Computation Costs.
- The data owner can perform dynamic operations of the files

Advantages of Proposed Methods:

- Here we focus on how a broker can help a group of customers to fully utilize the volume discount cost strategy offered by cloud service providers(CSP) through cost-efficient online resource scheduling.
- We present a randomized online stack-centric scheduling algorithm (ROSA) and theoretically prove the lower bound of its competitive ratio.
- Here using this (ROSA) algorithm we add the cost efficient system using here directly user can select discount offers without cloud broker involvement.

Feasibility Study

Feasibility study is an important phase in the software development process. It enables the developer to have an assessment of the product being developed. It refers to the feasibility study of the product in terms of outcomes of the product, operational use and technical support required for implementing it.

Feasibility study should be performed on the basis of various criteria and parameters.

The various feasibility studies are:

- Operational feasibility
- Technical feasibility
- Economic feasibility
- Feasibility Report

Operational Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being

placed on the client. The developed systemmust have a modest requirement, as only minimal or null changes are required for implementing this system.

Technical Feasibility

The technical issue usually raised during the feasibility stage of the investigation includes the following:

- Does the necessary technology exist to do what is suggested?
- Do the proposed equipment's have the technical capacity to hold the data required to use the new system?
- Will the proposed system provide adequate response to inquiries, regardless of the number or location of users?
- Can the system be upgraded if developed?
- Are there technical guarantees of accuracy, reliability, ease of access and data security?

Economic Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Software Requirement Specification

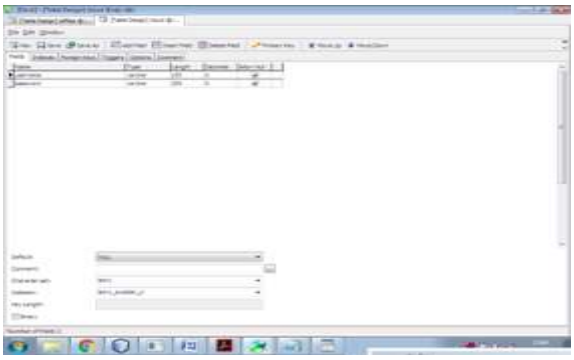
- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

Hardware Requirements

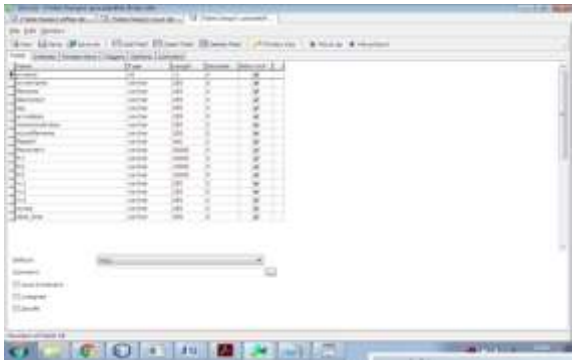
- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

III. DATABASE SCHEMES

1. CSP Login

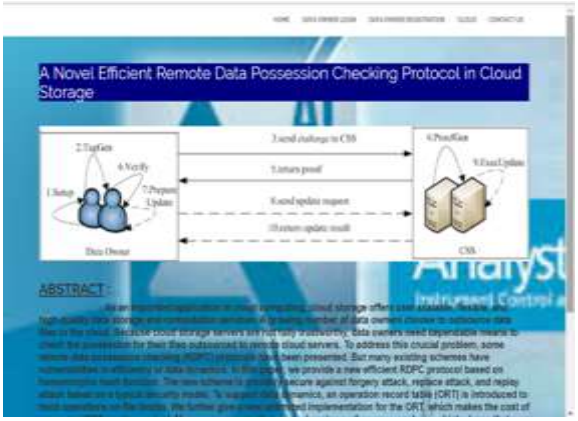


3. Data Owner Request



IV. OUTPUT SCREEN

1. Home page



2. Data owner Registration page

3. Login page

4. Cloud home

5. cloud view data owner request

6. cloud view data owners

7. Data Owner update request

8. Data Owner Home

9. Upload Files

10. view file

11. Data Possession challenge

12. Proof of verification

13. Dymaic operation

14. Download file

V. CONCLUSION

Files outsourced to remote server and propose an efficient secure RDPC protocol with data dynamic. Our scheme employsa homomorphism hash function to verify the integrity for the files stored on remote server, and reduces the storage costs and computation costs of the data owner. We design a new lightweight hybrid data structure to support dynamic operations on blocks which incurs minimum computation costs by decreasing the number of node shifting. Using our new data structure, the data owner can perform insert, modify or delete operation on file blocks with high efficiency. The presented scheme is proved secure in existing security model. We

VI. FEATURE ENHANCEMENT

structure in terms of block updates, we conduct another 'insertblocks' experiment on 1GB file. The size of block is set to be16KB, the total count of blocks is 65536. We realize the ORT by array, linked list and our hybrid data structure respectively. Based on these three types of ORT, we frequently insert blocks to random positions of the file. We run the experiments 1000 times for each condition, the average time cost is shown in Fig9. It notes that we set the length of sub-list in our new hybrid structure to 100.As observed, with the increasing number of inserted blocks, the time cost of the two traditional implementation for ORT(array and linked list) [18, 25] is almost increasing linearly while our new method keeps nearly constant at a very low level. Thus, our scheme has great advantages compared with the other two. In addition, as well known, MHT is also used to support dynamic operations for RDPC [17, 19]. However, to insert or delete blocks, it needs to first find the precise position of the block in MHT and then reconstruct the MHT tree. Besides, the hash values of the new block node and all the leaf nodes whose path changes after block operations should be recalculated. It is easy to prove that MHT will cost greater overhead even than array for these dynamic block operations [43]. Thus, our method is the most efficient one.

REFERENCES

[1] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic,"Cloud computing and emerging IT platforms: Vision, hype, and reality fordelivering computing as the 5th utility," Future Gener. Comp. Sy., vol.25, no. 6, pp. 599 – 616, 2009.

[2] H. Qian, J. Li, Y. Zhang and J. Han, "Privacy preserving personal health record using multi-authority attribute-based encryption with

revocation," Int. J. Inf. Secur., vol. 14, no. 6, pp. 487-497, 2015.

[3] J. Li, W. Yao, Y. Zhang, H. Qian and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2520932.

[4] J. Li, X. Lin, Y. Zhang and J. Han, "KSF-OABE: outsourced attribute-based encryption with keyword search function for cloud storage," IEEE Trans. Service Comput., DOI: 10.1109/TSC.2016.2542813.

[5] J. Li, Y. Shi and Y. Zhang, "Searchable ciphertext-policyattribute-based encryption with revocation in cloud storage," Int. J.Commun. Syst., DOI: 10.1002/dac.2942.

[6] J.G. Han, W. Susilo, Y. Mu and J. Yan, "Privacy-Preserving DecentralizedDKiesytr-iPboultiecdy SAystttreimbust,e v-Bola. s2e3d, nEon.1c1ry, pptpio. n2,1"5 0IE-2E1E62 ,T 2r0an1s2a ctions on Parallel and