International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Resource Allocation Using Optimized Data Stack Technique in Cloud

[1]N. Sureshbabu, [2]Dr. R. Pragaladan, [3]T Kannadasan,

Submitted: 03/02/2024 **Revised**: 11/03/2024 **Accepted**: 17/03/2024

Abstract: A wide range of advantageous features, including resource pooling, rapid elasticity, approximated services, on-demand self-services, and more, have made cloud computing extremely popular. But distributing resources securely among users with better authentication and privacy is a difficult problem in cloud networks. Thus, for the equitable exploitation of storage resources, an effective cloud resource design is suggested in this work. The information is kept up to date, organized, and available to authorized users with enhanced allocation properties that remove internal dangers. By supplying a unique storage key, the Optimized Data Stack (ODS) encryption technique locates the right storage site and efficiently allocates resources. The suggested method gives users immediate access to storage sites while offering high privacy and enhanced secrecy. Using Visual C#, the simulation is run, and the results show that the suggested method allocates resources quickly while making effective use of cloud server storage.

Keywords*: Resource Allocation, cloud computing, cloud environment*

1. INTRODUCTION

The information technology (IT) sector and a number of companies, such as youtube, dropbox, amazon are greatly impacted by cloud computing. These companies work hard to provide more cost-effective, secure, and efficient cloud services. Moreover, in an effort to optimize the benefits of cloud computing, IT companies are rebuilding their business services [1].Compute-intensive applications in cloud computing require more processing and memory capacity than networking resources. Furthermore, relative to processing power, network-intensive applications demand more networking bandwidth, which could result in unexpected traffic in the cloud system [2].

Some cloud applications require on-demand resource allocation from cloud service providers in order to handle unexpected spikes in incoming user traffic. In order to meet various needs, cloud service providers must effectively allocate and provision resources in the data center. Through the aid of the migration process, enterprise cloud systems' efficient resource allocation helps enterprises boost their returns on investment [3].The term "resource allocation and provisioning" in cloud systems describes the gathering, application, and run-time administration of hardware and software resources. Estimating the precise amount of resources required for the completion of a given workload in order to enhance resource utilization and provide financial benefits while also improving user experience with the application is a major challenge in resource provisioning of cloud service providers [4].

However, in a cloud environment the resources, like CPU, storage, and bandwidth, are diversified. To tackle this, multidimensional approaches are adopted for resource allocation. A multidimensional resource allocation is not potent in huge solution space as well as demands the utilization of a heuristic algorithm. In addition, these allocation schemes estimates the resource's average unit price with the classification of resources considering user demand. Anyway, multi-dimensional allocation concepts faced serious problems because of the absence of incentives and fairness [5].

Moreover, dynamic resource allocation is used, which is particularly laborious in an online setting where decisions must be made quickly to achieve the long-term objective of reducing allocation and reconfiguration expenses over time. Despite forecasting the workload or resource pricing in the future, a resource allocation decision must be made for the current time period while handling workload flash crowds [6]. By efficiently allocating computational and network resources, these allocation strategies lower the overall system latency. They choose the right node and network element pair that can process the current task to a satisfactory degree while minimizing the total delay, taking into account the system and network link load conditions at the time [7].

[1]*Assistant Professor, PG and Research Department of Computer Science Rajah Serfoji Government College, Thanjavur*
sureshbabunagarajan@yahoo.co.in
[2]*Assistant Professor & Head, Department of Computer Science, Sri Vasav College, Erode,*
pragaladanr@gmail.com
[3]*Associate Professor of Computer Science, Thanthai Periyar Government Arts and Science College (Autonomous)*
tkdasan33@gmail.com

However, migrating legacy software to the cloud can be challenging. Doubts have been raised if the cloud users can trust the cloud networks to protect the data and if it can avoid the unauthorized exposure of sensitive or private information. Moreover, the cloud networks can suffer from threats affecting the security [8]. Therefore, the adoption of the cloud-based security techniques is mandatory. To address this issue, the security of the cloud network can be assured with a trusted concept. Several existing methods analyze the trust concepts with respect to the security of the cloud networks [9].

In the existing security control model, the cloud can only assume the data category a user will output as well as utilize in functional stage of the cloud service; hence, the cloud is not aware of the extra security necessities as well as security controls adopted for safe guarding user's data. Users should know the variations in security assessment of the cloud, specifically with the demand to possess transparent view in the cloud service attained [10].The cloud should provide security as well as availability of their data and services, and demonstrate compliance with present security concepts. Estimating the security of cloud is a tedious process yet it provides speeding up the cloud adoption functioning by offering sufficient as well as transparent information regarding security of the provided services to customers and supporting their comparison in decision making process [11].

For providing security in cloud networks, it is important to store as well as exploit outsourced data in a secured as well as potent way. To protect data privacy as well as control, data is generally encrypted before outsourcing, resulting in challenging effective utilization. Specifically, indexing as well as searching the outsourced encrypted data is a serious issue [12].Hence, it is necessary to introduce a privacy aware authentication procedure that permits users for accessing different services from specific service providers by utilizing single private key or password [13].Several privacy-preserving public auditing protocols for regenerating-code-based cloud storage were proposed but they do not provide improved security features i.e., the proxy surrogated by data owner may forge an authenticator for any data block, which is evidently beyond the proxy's allowable capability [14]. Therefore, it is necessary to build an effective cloud model which ensures the secured access as well as transmission of data, and provides privacy protection for data information [15].

In this paper, a secured resource allocation is proposed in cloud which provides high throughput and improved data confidentiality. An efficacious Optimized Data Stack (ODS) algorithm is utilized which consumes minimal time as well as efficient storage.

2. PROPOSED METHODOLOGY

The proposed architecture is based on the group cloud model, which includes a set of organizations. Cloud architecture is a model in and committed users throughout the network on demand or prompted action. It requires an efficient allocation of data with improved classification and distribution property. An effective cloud resource architecture is suggested as a solution. The main elements of the suggested cloud resource architecture are shown in Figure 1.

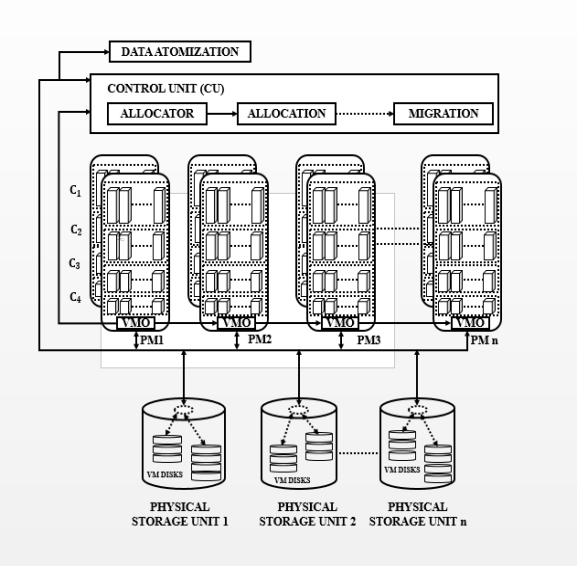

Figure 1: Proposed cloud resource architecture

The proposed architecture comprises of the following components,

a) Virtual Machine Observer (VMO)
b) Data atomization
c) Allocator
d) Physical storage unit (PSU)
e) Virtual machine disks

Virtual Machine Observer (VMO)

The physical cloud storage units are regulated by the VMO to monitor the storage abilities of each VMs inside the physical storage units. The information about the consumption of data are gathered by VMV and send to the control unit. The information consists of the available storage capacity.

Data atomization

The data to be stored in the virtual machine disks in the PSU are atomized into stacks as shown in figure 2. This atomization process is performed by considering the parameters like the number of data stack, size of each data stack as well as storage area in the data center. Each

data package received by atomization is of dynamic size.

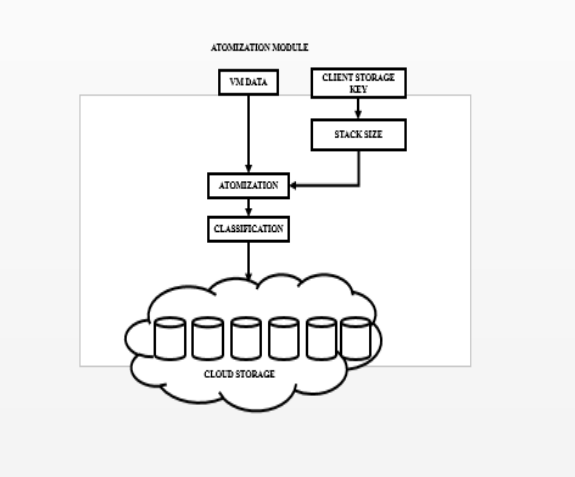

Figure 2: Atomization model of the proposed system

Allocator

The allocator performs the allocation of data packages and this allocation corresponds to the physical storage unit. The allocator efficiently allocates the incoming data into the PSUs. The PSUs are combined together to form a common storage for incoming data and is further divided into virtual blocks for the redirection of data stacks. The data to be saved in the cloud storage is allocated depending on its size to equal the storage size.

The advantages of this efficient resource allocation are given as follows:

a) Increased throughput due to the evenness in the data storage
b) It adopts time sharing as well as parallel computing property and hence the cloud resource allocation with large number of users is possible offering minimal congestion.
c) The data stacks are located directly by the user utilizing specific storage passwords. The storage locations of the data stacks are unaware and this results in secured allocation and storage of data. The proposed architecture offers high security by providing improved data confidentiality and privacy due to the placement of data stacks in separate hardware of the cloud network.

Proposed Technique: Optimized Data Stack

The resource allocation in cloud networks can be efficiently performed by adopting an encryption algorithm. Hence, an Optimized Data Stack algorithm (ODS) is proposed which performs efficient allocation of data. The basic operations of the proposed ADS algorithm are given below,

a) The data is evenly distributed along the storage area which reduces the overload condition.
b) It accurately identifies the data size and searches the appropriate storage location which consumes less time in data allocation.
c) The users will be provided with individual storage key which in turn improves the data integrity level much better than previous ones.
d) The algorithm offers high confidentiality by enabling the direct access of storage locations by user. The data is not stored completely in a single location, instead the user's key divides the data into data stacks and stores it across the storage units. This improves the privacy of an individual's information in the cloud networks.

The step by step sequence for the proposed algorithm is given below,

Input: U_{KEY}→ User key

U_D→ User data

Output: D_{LOC}→ Data stack location

N_U→ Number of units

T→Time taken for data storage

1) Initial N←0, D_{stacks}←[], $UnitCount_{alloc}$←0, $Unit_{alloc}$←null
2) Load U_D
3) N←GENERATINGNUMBEROFSTACKS(U_{KEY})
4) D_{stacks}←ATOMIZATION(N,U_D)
5) For each d∈D_{stacks}
6) $Unit_{alloc}$←ALLOCATIONALGORITHM(d)
7) Add d location into D_{LOC}
8) $UnitCount_{alloc}$+ +
9) End for
10) N_U←$UnitCount_{alloc}$
11) Return D_{LOC}, N_U, T

Generating the number of stacks:

Input: U_{KEY}→6 digit user key

Output: N_{stacks}→Number of stacks

1) If U_{KEY}= 6 digit then return null
2) Initial D_{binary}←0, D_{list}←[],$D_{crossover}$←[]
3) New_{KEY}←SUBTRACT(α,U_{KEY}) /*α is the higher value formed from 6-digit*/
4) Job_{code}←RANDOM(MIN,MAX)
5) New_{KEY}←ADDITION(New_{KEY},Job_{code})
6) D_{list}←TOLIST(New_{KEY})
7) $D_{crossover}$←CROSSOVER(β,D_{list}) /*Number of crossover operations on the mutated D_{list}*/
8) D_{binary}←CONVERT2BINARY($D_{crossover}$)
9) N_{stacks}←NUMBEROFONES(D_{binary})
10) Return N_{stacks}

Allocation Process:

Input: D_{stacks}

Output: D_{LOC}

1) Initial N←0,P_S←storage pool, $Unit_{alloc}$←null
2) Divide P_S into ρ blocks
3) C_ρ←GENERATECLASSTYPE(D_{stack},ρ)
4) $Unit_{alloc}$←SELECTBINCLASS(C_ρ)
5) Return $Unit_{alloc}$

Thus the proposed algorithm follows a unique approach for allocating units in the cloud network. The allocation performed consumes minimal time and adopts the storage in an efficient manner.

3. EXPERIMENTAL RESULTS

The overall simulation package is a typical collection of classes generated to do sequential processes to obtain the desired goal. Each class denotes the components in our designed architecture. The important components are,

a) Allocation unit
b) Control unit
c) Machine manager unit

The other integral portion of this architecture is the incoming storage demands from the clients of the cloud. The data is to be stored in the cloud storage server so that there occurs no extra depletion in resources offering secured allocation. The simulation results indicated that less number of units are utilized and the time consumed by the algorithm to allocate data is much less compared to other existing algorithms. The figure below indicates the time consumed by the proposed approach for allocating the VM data of users in the cloud storage location. When compared to the existing approaches like first fit algorithm, best fit algorithm, the proposed algorithm showed efficient results.

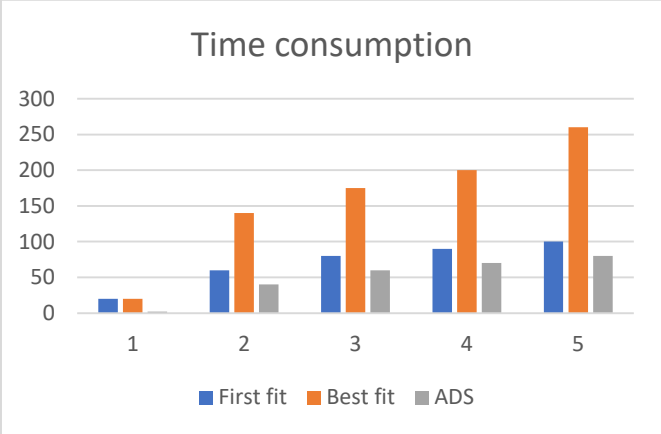

Figure 3: Comparison of time consumption

The figure below depicts the utilization of resources by the number of units used to allocate the data. The proposed approach revealed efficient results in terms of allocation when compared to existing approaches.

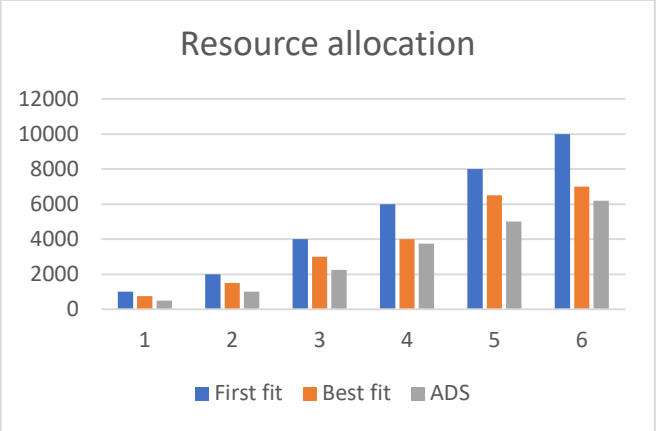

Figure 4: Comparison of resource allocation

The table below shows the number of servers utilized by the first fit algorithm, best fit algorithm and the proposed algorithm. It clearly indicates the efficient utilization property of the proposed approach.

	No. of servers in first fit algorithm	No. of servers in best fit algorithm	No. of servers in ADS algorithm
100	999	791	586
200	1966	1597	1233
400	4014	3214	2413
600	5963	4083	3641
800	7899	6450	5000
1000	10049	7109	6289

Table 1: Number of servers

From the table it is clear that even though the number of users increased from 100 to 1000, the count of servers adopted by the proposed approach is minimum when compared to existing ones. The comparison graph of the proposed algorithm with the existing ones is shown below

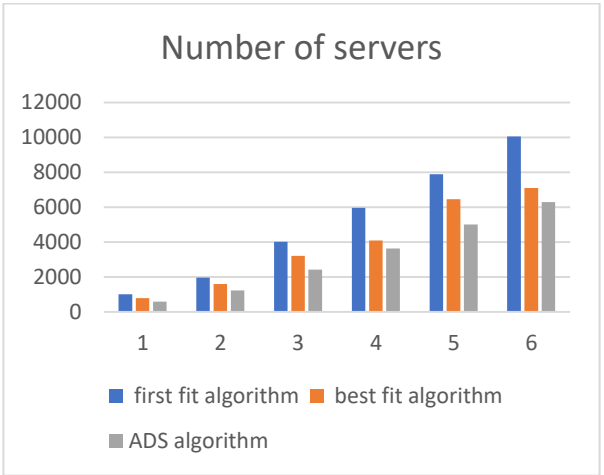

Figure 5: Comparison of the number of servers

Thus the proposed algorithm provides robust security with enhanced data confidentiality, privacy as well as integrity and allocates the resources among cloud users in an efficient manner. Due to the atomization of data into stacks in this approach, even access of data is attained without overloading issues.

4.CONCLUSION

Efficient resource allocation with improved privacy and data confidentiality is a serious concern in cloud networks. In this paper, a resource allocation architecture is introduced for even utilization of resources eliminating internal threats. An efficient Optimized Data Stack algorithm is proposed which adopts an exclusive concept for unit allocation in cloud networks. The functioning of the algorithm is simulated in Visual C# and the results demonstrated that the proposed approach consumed less time utilizing better storage. Future works may concentrate on the operation of the proposed approach in real time cloud networks.

REFERENCES

[1] SiqianGong;BeibeiYin;ZhengZheng;Kai-YuanCai,2019, "Adaptive Multivariable Control for Multiple Resource Allocation of Service-Based Systems in Cloud Computing", IEEE Access, Vol: 7, pp: 13817 – 13831.

[2] JungminSon;RajkumarBuyya, 2019, "Priority-Aware VM Allocation and Network Bandwidth Provisioning in Software-Defined Networking (SDN)-Enabled Clouds", IEEE Transactions on Sustainable Computing, Vol: 4, No: 1,pp: 17-28.

[3] JyotiskaNathKhasnabish;MohammadFirojMithani; Shrisha Rao, 2017, "Tier-Centric Resource Allocation in Multi-Tier Cloud Systems", IEEE Transactions on Cloud Computing,Vol: 5, No: 3, pp: 576-589.

[4] RehanaBegam;WeiWang;Dakai Zhu, 2020, "TIMER-Cloud: Time-Sensitive VM Provisioning in Resource-Constrained Clouds",IEEE Transactions on Cloud Computing, Vol: 8, No: 1, pp: 297-311.

[5] Wei Wei;XunliFan;HoubingSong;XiumeiFan;Jiachen Yang, 2018 , "Imperfect Information Dynamic Stackelberg Game Based Resource Allocation Using Hidden Markov for Cloud Computing",IEEE Transactions on Services Computing, Vol: 11, No: 1, pp: 78-89.

[6] Lei Jiao;Antonia Maria Tulino;JaimeLlorca;YueJin;Alessandra Sala, 2017, "Smoothed Online Resource Allocation in Multi-Tier Distributed Cloud Networks, IEEE/ACM Transactions on Networking, Vol: 25, No: 4, pp: 2556 – 2570.

[7] SuchintanMishra;Manmath Narayan Sahoo;SambitBakshi;Joel J. P. C. Rodrigues, 2020, "Dynamic Resource Allocation in Fog-Cloud Hybrid Systems Using Multicriteria AHP Techniques", IEEE Internet of Things Journal,Vol: 7, No: 9, pp: 8993 – 9000.

[8] Dan Gonzales;Jeremy M. Kaplan;EvanSaltzman;ZevWinkelman;Dulani Woods, 2017, " Cloud-Trust—a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds,IEEE Transactions on Cloud Computing, Vol: 5, No: 3, pp: 523-536.

[9] Xiang Li;QixuWang;XiaoLan;XingshuChen;NingZhang; Dajiang Chen, 2019, "Enhancing Cloud-Based IoT Security Through Trustworthy Cloud Service: An Integration of Security and Reputation Approach", IEEE Access,Vol: 7, pp: 9368-9383.

[10] Jesus Luna;AhmedTaha;RubenTrapero;NeerajSuri,2017, "Quantitative Reasoning about Cloud Security Using Service Level Agreements",IEEE Transactions on Cloud Computing, Vol: 5, No: 3, pp: 457-471.

[11] TalalHalabi;Martine Bellaiche,2020, "Towards Security-Based Formation of Cloud Federations: A Game Theoretical Approach",IEEE Transactions on Cloud Computing, Vol: 8, No: 3, pp: 928-942.

[12] AbirAwad;AdrianMatthews;YuansongQiao;Brian Lee, 2018, "Chaotic Searchable Encryption for Mobile Cloud Storage,IEEE Transactions on Cloud Computing, Vol: 6, No: 2, pp: 440-452.

[13] Qi Jiang;JianfengMa;Fushan Wei, 2018, "On the Security of a Privacy-Aware Authentication Scheme for Distributed Mobile Cloud Computing Services, IEEE Systems Journal, Vol: 12, No: 2, pp: 2039 – 2042.

[14] JindanZhang;RongxingLu;BaocangWang;Xu An Wang, 2021, "Comments on "Privacy-Preserving Public Auditing Protocol for Regenerating-Code-Based Cloud Storage",IEEE Transactions on Information Forensics and Security, Vol: 16, pp: 1288 – 1289.

[15] FanyuKong;YufengZhou;BinXia;LiPan;Limin Zhu , 2019, "A Security Reputation Model for IoT Health Data Using S-AlexNet and Dynamic Game Theory in Cloud Computing Environment",IEEE Access, Vol: 7, pp: 161822 – 161830.