Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

Analysis Study for Optimization Methodologies in Cloud Architecture for Reliable Erp Solutions

[1]R. Gaverineni Siva Ratna Kiran, [2]Dr. Jammalmadaka Kodanda Rama Sastry

[1]Research Scholar, KL University, Green Fields, Vaddeswaram, Andhra Pradesh, India.
[2]Professor, KL University,Green Fields, Vaddeswaram, Andhra Pradesh, India.
*Corresponding Author : drjkrsastry@gmail.com

Abstract.
All the organizations go through the challenges in protecting their Data. While using cloud technology, it creates a tension between the enterprise and the executives in controlling the new modes of operations. The challenges faced in planning, contracting, and managing the services while using cloud must be deliberately address by the providers and clients so that these types of tensions can be solved. While sharing the data on cloud, data losses, delays and interruptions are occurring. For better outcome analysis of cloud structure and cloud problem studies are discussed in this paper.

Keywords: Cloud Computing, Cloud ERP, Cloud Threats, Failures and Security

INTRODUCTION:

Cloud Services has many advantages like liveliness, location independence and cost effectiveness which made a trend over the past decade. Many organizations and cloud providers are offering DaaS services which became common and trustworthy while keeping and sharing large files. Dropbox, Google Drive, Apple iCloud, and Microsoft OneDrive are few well-known industry applications.There are specific policies that each company will need to create on its own in order to accommodate and protect business functions, but there are other, more general recommendations that apply to anyone using the cloud. In order to get started when creating enterprise best practices, the Cloud Security Alliance offers a list of common policies and the Cloud Best Practices Network provides case studies to help build better long-term strategies. Few basic steps which can be followed by the organizations who are searching for a method to use cloud safely and for preventing data loss are discussed below.
Perform a cloud risk assessment:Cloud risk assessment is the process in which the companies need to take an account over all the cloud applications they are using and needs to check the location where their data are being stored in the network. This will help the IT decision-makers to develop ‘as is’ cloud assessment and to understand the process of it. For identifying the company’s current cloud footprint, the enterprise network must be surveyed after the process of inventory and should create a data flow map. After all these processes, a risk score must be given for each program and the level trust the company rates for all those service and process.Find any gaps between perceived security and actual security:In this step, any discrepanciesbetween regulatory compliance needs like PCI (Payment Card Industry)or HIPAA (Health Insurance Portability and Accountability Act) can be identified, and the businesses can find what is going on in the network. The issues can be easily identified and resolved when the areas that posses’ huge gaps are discovered by the decision makers.
Build a plan to combat shadow IT:Shadow IT, or unapproved programs usage by the employees is one of the major cloud security issue faced by the companies. An action plan could be created by the companies by the data collected through the previous steps to identify this issue and consulting legal, security and procurement specialists would also help them to overcome this issue.
Choose a cloud framework to deploy:A cloud platform that will meet all the necessary requirements could be finding when a comprehensive analysis of the enterprise’s needs is prepared. The suitable environment between a public, private or hybrid and the service provider who provides reliability, features and client servicemust be decided by the IT executives[10].

Challenges of Cloud Computing

In a Cloud Survey termed RightScale 2019, stated that 94% of IT organizations were utilizing cloud computing services in which 91% of them were utilizing public cloud (fig 1).
It comes along with some pros and cons yet, if proper technology is selected, the organizations will grow without any obstacles. Though Cloud computing is being an important technology of few organizations, it also comes with

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

few problems and it might be serious issues in some cases[11]. These issues are the major challenges in cloud computing.

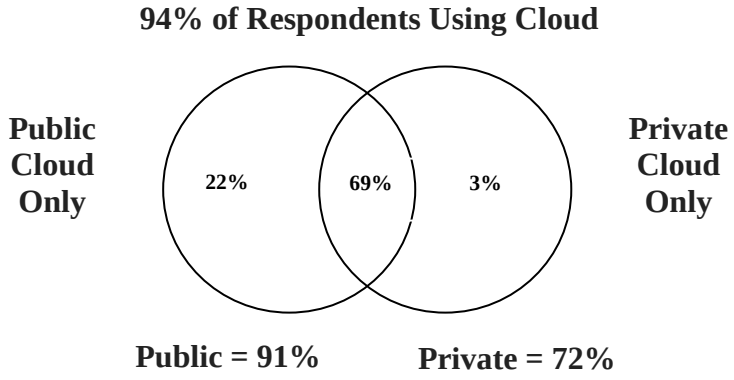


Fig No: 1 Average of Cloud Report

Benefits and Challenges of cloud ERP systems

Cloud computing had kept its feet firmly in software industry and in academic research also. With cloud computing, the user can avail availability, scalability, and flexibility in operations at various levels at very minimal running cost. It is a computing method through which general business community requirements can be satisfied. The applications, the hardware and software that delivers its services over the internet are termed has cloud computing. It provides it services in three different models and they are (fig 2): Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), Figure below shows the cloud service models.

Software as a Service (SaaS), mainly focus on the end user or the organization, where it delivers software applications to multiple users over the internet. Cloud ERP systems also comes under this category and it is discussed below.

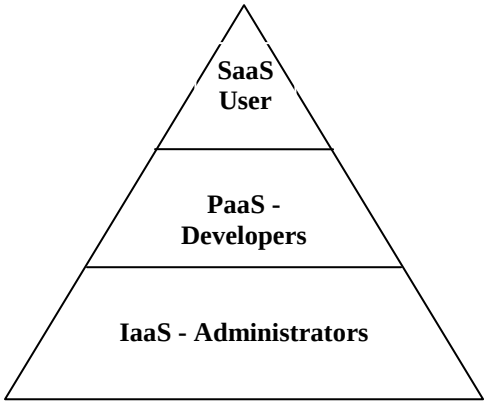


Fig No: 2 Cloud Service Models

Platform as a Service (PaaS) focus on the tools, services and platforms that required by the software developers which is known as middle ware. SaaS applications are build through it.

Infrastructure as a Service (IaaS) is required by the administration of the organization for receiving computing power hardware and software and it can be altered or upgraded according to the growth of its business.

Cloud ERP

Cloud ERP solutions are delivered as a Service model through the software. The characteristic features of Cloud computing influenced the ERP system to become Cloud based ERP system. The user can access this system via the user browser through the internet without getting connected to system in any physical mean. To overcome the issues like data delay and data loss are rectified by Load balancing.

There are two different load balancing approaches which are suitable for different criteria. They are static load balancing and dynamic load balancing algorithms. Static load balancing algorithms can assign the task to the nodes only based on the ability of the node. Which means it cannot assign the task to the node if the node does not

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

possess any prior knowledge based on its properties and capabilities for doing the new task. Whereas Dynamic load balancing algorithms possess the capability in capturing different attributes of nodes capabilities and network bandwidth. It can also be able to assign or reassign the tasks to the nodes dynamically depending on the features calculated before and during run-time.

Research has been made to understand various aspect of storage optimization for reducing the usage of space without making any compromise with consistent, reliable, and highly accessible data. Few relevant examples are provided below.

Related studyand failure detection approaches

[2]A load balancing algorithm utilizing virtual to physical machine mapping for the private cloud was proposed. The algorithm consists of a central scheduling controller and a resource monitor. It completes the task through 4 stages like accepting the request from the virtual machine, receiving the resource details through resource monitor, then the ability to handle the task is calculated before assigning the task followed by the task assignment and then the access is provided to the client.

[7]a dynamic load balancing algorithm for cloud computing was proposed by utilizing an existing algorithm called WLC (weighted least connection)[4]. In WLC, tasks are assigned to the node based on the number of connections available with that node yet it will not consider the capabilities the node possesses regarding processing speed, storage capacity, and bandwidth. Whereas the proposed ESWLC (Exponential Smooth Forecast based on Weighted Least Connection) allocate the task based on an experience of node's CPU, memory, number of connections, load of disk occupation and it also decides the node that has to be selected based on exponential smoothing.

[6]Proposed an algorithm named as Load Balancing Min-Min (LBMM), it consists of three-level load balancing framework and also utilized the concept of the Opportunistic Load Balancing algorithm (OLB)[1]. OLB mainly focus on allotting the task to each node and keep them engaged yet it does not take the execution time into consideration. LBMM on the other hand rectified this issue by including three-layered architecture to the algorithm. In first level, request manager receives the task and assign it to one service manager who is in second level of LBMM. The service manager divides it into many subtasks to number of service nodes based on the attributes like remaining CPU space (freeness of the nodes), remaining memory, and the transmission rate so that the processing speed will become high.

[9]A full replication solution was proposed which was termed as BerryStore which focus on downloading small files from the cloud its maximum size is 10MB. In this solution there is only one directory entry in the cloud nodes as it groups many small files into one large file. The client is the main structure of this solution along with, Name Server and DataServer. When the client request for the file, NameServer locates the file and the client can download the file from DataServer where the real file data is available. Though the solution has good outcome it cannot be applied for large files.

[5]A solution that works for single and multicloud storage was proposed that reduces the effort in migrating the client data from one cloud to another. Yet when the files are saved on different clouds, it creates complex process.

[3]Author discussed about FD Module which is an essential utility of the fault tolerant framework. On the other hand AFD is Adaptive Failure Detection Framework used for identifying possible failures that are checked by the operators of cloud.

Villarreal-Vasquez et.al (2017) for establishing cloud systems with resiliency to an extent that they can alleviate failures to deliver continuous working of basic responsibilities. Forpermittingself-versatile SDN (Software Defined Network) reconfiguration with an MTD (Moving Target Defence) method, it depends on dispersed checking of cloud service/VM conduct and regular stimulating of the related cloud assets.

Cloud Computing Failures that Shocked the World

Cloud computing failure occurs even to the prominent cloud providers all over the world. It might be a small service disruption or a loss of customer data, even the most popular vendors faced these kinds of issues.

Amazon Web Services (AWS): The market leader had a major hit which created tension all around. The reasons started from power outages to data centres which led to human errors. It created a major drawback for personal and professional lives.

Salesforce goes down: The Silicon Valley NA14 instance of Salesforce.com went offline on May 9th, 2016 which was not rectified for a period of 24 hours. This made them to lose their customers and some hours of data. As a result, most of its workload moved to Amazon Web Services.

A bad Christmas for Netflix: Netflix faced a huge downtime in 2012, Christmas because of AWS's Elastic Load Balancing service issue. Which spoiled the Christmas celebration of customers who depends on the streaming on Netflix. Two years later, during an AWS update Netflix rebooted 218 of its production nodes in which 22 failed to

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

reboot.

Microsoft Azure goes bust: On November 18, 2014, Because of the software updates aimed at increasing the performance, a massive outage hit the Azure Storage Service and a similar one happened again in December 2015.

Dyn sees a bad day: A series of Distributed Denial of Service (DDoS) attacks occurred on October 21, 2016 which made lots of websites and their businesses were smacked, for example those of Airbnb, Twitter, Amazon, Ancestry, Netflix, and PayPal. The practical threat of large-scale Internet of Things (IoT) attacks made the world to be alert to face these kinds of challenges.

The Office 360 joke: In Microsoft's Office 365, the email services went offline for more than 12 hours of their clients. Similar incidence happened from 2015 to 2016 which created a joke saying that Office 365 is indeed Office 360, with an average downtime of five days off a year.

Healthcare takes a hit: Due to poor design, lack of resources and demand exceeding supply, frequent website crashes occur in HealthCare.gov. Cloud left the important government service that concerns the public health.

Table No: 1 Some examples of features

Feature	Type	Description
Update Domain	Spatial	The domain where nodes share same update setting.
Memory Usage	Temporal	Memory consumption.
Disk Sector Error	Temporal	Sector errors in a disk drive
Service Error	Temporal	Error counts from a deployed service.
Rack Location	Spatial	The location of the rack the node belongs to
Load Balance Group	Spatial	The location of the rack the node belongs to
IOResponse	Temporal	I/O Response time
OSBuildGroup	Spatial	The group where nodes have the same OS build.

Analysis of the Cloud Secure

The cloud or multi-cloud environments security must be continuously ensured by the organizations for the purpose of their data security. The major difficulty faced by the organizations is that they must provide the same security control in the cloud environment that they did for their legacy, data centre environment. In this even if the cloud providers takes responsibility in protecting the data in the first level, it is the responsibility if the organization to protect them in the second level which can protect its data.

Security of Data

1. Insufficiency of Resources and Expertise
2. Complete Governance over IT Services
3. Cloud Cost Management
4. Dealing with Multi-Cloud Environments
5. Compliance
6. Cloud Migration
7. Vendor Lock-In
8. Unformed Technology
9. Cloud Integration

Cloud computing security issues

Cloud computing comes along with some rare security and challenging issues. The Cloud service providers consider this has shared responsibility of both Cloud service providers and the clients. While cloud providers take care of cloud protection it is the responsibility of the clients about the data they transfer through cloud (fig 3).

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

Shared Responsibility Model for Security in the Cloud			
On-Premises (for reference)	**IaaS(infrastructure-as-a-service)**	**PaaS (Platform-as-a-service)**	**SaaS (Software-as-a-service)**
User Access	**User Access**	**User Access**	**User Access**
Data	**Data**	**Data**	**Data**
Applications	**Applications**	**Applications**	Applications
Operating System	**Operating System**	Operating System	Operating System
Network Traffic	**Network Traffic**	Network Traffic	Network Traffic
Hypervisor	Hypervisor	Hypervisor	Hypervisor
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Fig No: 3 Shared responsibility for security between cloud providers and their customers

There are security risks in cloud computing mainly related to the cloud data security like lack of visibility to data, inability to control data, or theft of data in the cloud. Most of them come as the result of the data the customers' stores in it. Few analyses of the cloud security issues that many organizations experienced in SaaS, IaaS, and private cloud are mentioned below.

Top 5 Private Cloud Security Issues

1. Lack of consistent security controls spanning over traditional server and virtualized private cloud infrastructures
2. Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance
3. Lack of staff with skills to manage security for a software-defined data center (virtual compute, network, storage)
4. Incomplete visibility over security for a software-defined data center(virtualcompute, network, storage)

Advanced threats and attacks

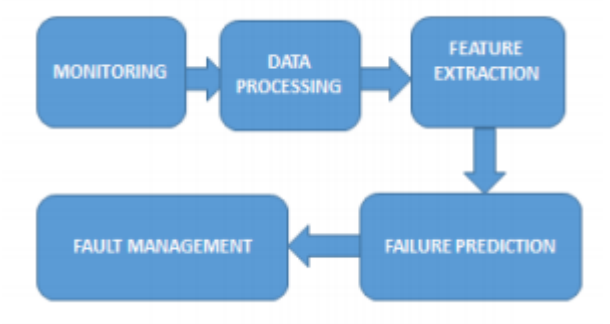
During the decision-making process of allocating resources to a public vs. private cloud, private cloud providers serve fine tuned control where additional levels of protections are available that makes it overcome some of the drawbacks, they face in cloud computing. The organization can do abstraction of controls and reduce the complexity as the cloud providers serves with fine-tuned control. This helps in unifying public and private cloud platforms across physical, virtual, and hybrid environments.

Proposed Techniques

Few advanced technologies are available in cloud computing services like artificial intelligence, virtual reality,machine learning, augmented reality, andadvanced big data analytics. These advanced technologies sometimes fail (fig 4) in fulfilling the organizational values in terms of dependability, usability, and functionality. Five stages of failure prediction model is listed below.

1. Monitoring and storing the system and application metrics
2. Processing data to structured formats containing their spatial and temporal information
3. Extracting relevant features from data
4. Predicting failures using machine learning model
5. Failure remediation management based on the predicted results

Data processing, feature extraction and failure prediction are focussed, and remediation of failure is given based on the prediction results to future work.



Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

Fig No: 4 Proposed Failure Prediction Method

Alleviate the threads risk: It is important to observe and examine the threats because it is not possible to certify that every cloud provider meets all the standards for security and risk. Because not every organization has the capabilities to rectify these types of threats. Two types of threats are being an obstacle for implementing cloud solutions and they are internal threats that come within the organizations and external threats that come from the professional hackers.

Unauthorised service provider: Cloud computing is not a familiar concept for many organizations, and it is difficult for them to verify the cloud providers authorization. To verify the service provider, few criteria can be seen before trusting any cloud provider. They must possess some years of experience in this field and they should not possess any negative records in the past and trusted clients reviews will also help the organization in choosing the provider.

Hacking of brand: Hacking is one of the major risks that comes along with Cloud computing. Professional hackers may be able to break all the securities and steal the data from the organization. If any action taken against a particular issue might affect the other clients who are under that cloud provider.

Table No: 2 Network-related Cloud Threats (Confidentiality-C, Integrity-I and Availability-A)

Thread	***Vulnerability***	***C***	***I***	***A***
$Maliciousprobesorscans$	$Openports$ $UnavailableormisconfiguredIDS$	•		
$Cross$ $-VMattackviasidechannels$	$Multi-tenancy$	•	•	•
$Dataleakageonup/download,$ $intra-cloud$ $Man-in-the-Middle$	$Communicationencrptionvulnerabilities$ $Weakauthenticationmechanism$ $Poorpatchmanagement$	•	•	•
$DenialofService$	$Poorsystemconfiguration$ $Inadequateresourcefiltering$ $Weakpoliciesforresourcecapping$			•
$Floodingattackvia$ $bandwidthstarvation$ $Fraudulentresourceconsumtio$	$BandwidthUnder-provisioning$ $ExploitationoftheCloudPricingModel$			•
$Cross-sitescripting$	$Insertionofuncheckeddatainrestricedsyste$ $Lackofmonitoringmechanism$	•	•	•
$Cross-siterequestforgery$	$Weakauthenticationormonitoringmechani.$ $Insertionofunauthorizedcommandsinthebr$	•	•	•
$Cookiemanipulation$	$Lackofhashestoprotectcookie$ $Weakencrytionmechanism$	•	•	•
$Cookiereplayattack$	$Insecuresystemdatabase$ $Lackoftimestamp$	•	•	

Table No: 3. Organizational Cloud Threats

Thread	***Vulnerability***	***C***	***I***	***A***
$Lossofgovernance$	$Unclearrolesandresponsibilities$ $SLAclauseswithconflictingpromisestostakeholde$ $Auditorcertificationnotavailabletocustomers$ $Nocontrolonvulnerabilityassessmentprocess$ $Certificationschemesnotadaptedtothecloud$ $Lackofinformationonjurisdictions$ $Lackofcompletenessandtransparencyintermsof$	•	•	•

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

$Lock-in$	$Poorproviderselection$ $Lackofsupplierredundancy$ $Lackofcompletenessandtransparencyintermsof$			•
$Non-compliance$	$Auditorcertificationnotavailabletocustomers$ $Lackofstandardtechnologiesandsolutions$ $Certificationschemesnotadaptedtothecloud$ $Lackofinformationonjurisdictions$ $Lackofcompletenessandtransparencyintermofu$	•	•	
$Serviceterminationorf$	$Poorproviderselection$ $Lackofsupplierredundancy$			•
$Supplychainfailure$	$Cross$ $-cloudapplicationscreatinghiddendependency$ $Poorproviderselection$ $Lackofsupplierredundancy$	•		•
$Conflictsbetweencusto$ $hardeningproceduresa$ $cloudenvironment$	$Lackofcompletenessandtransparencyintermsof$ $SLAclausewithconflictingpromisestostakeholde$ $Unclearrolesandresponsibilities$	•		•

Table No: 4 System or Data-oriented Cloud Threats

Thread	***Vulnerability***	***C***	***I***	***A***
$Bruteforceattacks$ $Dictionaryattacks$ $Priviegeescalation$	$Weakpasswordpolicy$ $Weakencrytionorauthentication$	•	•	•
$Bufferoverflows$	$Applicationvulnerabilities$	•	•	•
$Managementinterfacecomprom$	$Remoteaccess$ $SystemorOSvulnerabilities$ $Applicationvulnerabilitiesorpoorpatchm$	•	•	•
$Filesystemorregistrytampering$	$Poormanagementofpriviegedistribution$ $Weakprotectionmechanism$	•	•	•
$Serviceenginecompromise$	$Hypervisorvulnerabilities$ $Lackofresourceisolation$	•	•	•
$Dishonestcomputationinremotes$	$Lossofphysicalcontrolofdataandapplica$		•	
$Connectionpooling$	$Weakauthentication$	•	•	•
$Physicalthreats(theft,vandalis$	$Unreachabledatastoragelocation$ $Weakphysicalsecuritymeasures$ $Unknownriskprofile$	•	•	•
$Data disclosure/Leakag e/Insid$	$Weakencryptionorauthentication$ $Insidersontheproviderside$	•		

Data loss/Manipulation	*Lossofphysicalcontrolofthedata Poorintegrityorbackupcontrols*		•	•

Recovery of lost data: Data loss is one of the common issues faced in the cloud services and every cloud provider is responsible for setting a proper infrastructure for having the data backup so that it can be retrieved when anything gets lost. It's better to have at least of two different backup sites to manage this issue.

Data Portability: Data portability must be ensured by the cloud provider with proper contract for it. Every client expects to have control over the migration of the cloud, and many have dissatisfaction in this issue. Even they must possess an updated copy of data to get switched if there are any urgent requirements.

CONCLUSION

Cloud computing faces many new challenges in risk assessment which includes less secured boundaries, an unknown risk profile that is affected by new threats, the assessment of a dynamic environment and multiple origin points (the provider, the technology itself, other co-tenants, etc.). When such assessments are made, the level of trust over the cloud service provider can be improved. In this paper that factors that rectifies the risk when mitigating to the Cloud, along with a list of possible threats that could be faced while using cloud computing are discussed.

CONFLICTS OF INTEREST:

The author have declared no conflicts of interest

ACKNOWLEDGEMENTS

I'm R. Gaverineni Siva Ratna Kiran, Completed Bachelor of Commerce in passed out year of 2000, First class at SRI balaji degree college, Acharaya Nagarjuna, University, Vijayawada, Andhra pradesh. MS(IT) completed at Bharathidasan university, passed out on 2001-2003, Bishop Heber college, Tiruchirappalli, Tamilnadu. M.Tech CSE, Acharaya Nagarjuna, University, Vijayawada, Andhra Pradesh, Passed out on 2010 with 74% and PG Diploma in Computer application 2000-2001 at Comtec India Pvt Ltd, Vijayawada with A Grade.This is to convey my interest in exploring the opportunity of being part of your elite team as a Trainer and Developer. With almost 18 years of successful career in IT Training & Development.

REFERENCES

[1] A. Sang, X. Wang, M. Madihian, and R. D. Gitlin, "Coordinated load balancing, handoff/cell-site selection, and scheduling in multi-cell packet data systems," Wireless Networks, vol. 14, no. 1, pp. 103–120, 2008.

[2] J. Ni, Y. Huang, Z. Luan, J. Zhang, and D. Qian, "Virtual machine mapping policy based on load balancing in private cloud environment," in Proceedings of the International Conference on Cloud and Service Computing (CSC '11), pp. 292–295, IEEE, December 2011.

[3] Liu, J., Zhou, J., &Buyya, R.: Software Rejuvenation Based Fault Tolerance Scheme for Cloud Applications. IEEE 8th International Conference on Cloud Computing.doi:10.1109/cloud.2015.164. (2015).

[4] R. Lee and B. Jeng, "Load-balancing tactics in cloud," in Proceedings of the 3rd International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC '11), pp. 447–454, IEEE, Beijing, China, October 2011.

[5] S. Srivastava, V. Gupta, R. Yadav, and K. Kant, "Enhanced distributed storage on the cloud," in Proceedings of the 3rd International Conference on Computer and Communication Technology (ICCCT '12), pp. 321–325, IEEE, Allahabad, India, November 2012.

[6] S.-C. Wang, K.-Q. Yan, W.-P. Liao, and S.-S. Wang, "Towards a load balancing in a three-level cloud computing network," in Proceedings of the 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT '10), pp. 108–113, July 2010.

[7] X. Ren, R. Lin, and H. Zou, "A dynamic load balancing strategy for cloud computing platform based on exponential smoothing forecast," in Proceedings of the IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS '11), pp. 220–224, September 2011.

[8] S. Kanaga Suba Raja, M.Hema,'An Optimal Algorithm to Improve Resource Utilization in Cloud Data Centre', International Journal of Engineering and Advanced Technology, ISSN: 2249 – 8958, Volume 9, Issue - 1,2019

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 95-103
Received 15 April 2021; Accepted 05 May 2021.

[9] Y. Zhang, W. Liu, and J. Song, “A novel solution of distributed file storage for cloud service,” in Proceedings of the 36th Annual IEEE International Computer Software and Applications Conference Workshops (COMPSACW '12), pp. 26–31, July 2012.

[10] A.Prasanth, S.Jayachitra, 'A Novel Multi-Objective Optimization Strategy for Enhancing Quality of Service in IoT enabled WSN Applications', Peer-to-Peer Networking and Applications, Vol.13, 2020, pp.1905–1920.

[11] A.Prasanth, S.Pavalarajan, 'Implementation of Efficient Intra- and Inter-Zone Routing for Extending Network Consistency in Wireless Sensor Networks', Journal of Circuits, Systems, and Computers, Vol.29, 2020

[12] Rahim, Robbi, S. Murugan, Reham R. Mostafa, Anil Kumar Dubey, R. Regin, Vikram Kulkarni, and K. S. Dhanalakshmi. "Detecting the Phishing Attack Using Collaborative Approach and Secure Login through Dynamic Virtual Passwords." Webology 17, no. 2 (2020).