International Journal of Knowledge Based Computer Systems
6 (1), June 2018, 07-11
http://www.publishingindia.com/ijkbcs/

Improving the Service Solutions on Hybrid Clouds at Edge Network Using Fuzzy Approaches

R. Poorvadevi[1*] and S. Ramamoorthy[2]
[1]Assistant Professor, Department of CSE, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, Kanchipuram, Tamil Nadu, India. Email: poorvadevi@gmail.com
[2]Assistant Professor, Department of CSE, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University, Kanchipuram, Tamil Nadu, India. Email: sriraram2@gmail.com

Abstract: So far in cloud computing environment, all the resources and services are used as an on-demand request basis from the client end. All typical service issues have been solved with the optimal cloud resource customization policies. The role of edge computing is enabling the data processing operations at the edge network which will operate in the cloud computing platforms. Due to increased amount of usage in the client location the proper devices need to be well connected with an internet. Edge mechanism is implemented in the real-time service based operation which will examine the upstream and downstream functional units will apply the real-time local data analysis in the data centre locations. The hybrid clouds will execute the service request form both the private cloud and public cloud users. These services and request based resources can be literally focused by the cloud service provider (CSP) and managed service provider (MSP) who will provide the cloud services uninterruptedly to the requested users. When the multiple services are executes in the edge network then the cloud vendor does not properly handle the services through the secured environment. Such kind of problem will lead the user to loss their control activities on the hybrid cloud solutions location. The proposed approaches of edge computing in hybrid cloud solutions are improving the service by applying the fuzzy logic control implementation factors. The cloud sim can be used as a simulator in the proposed model.

Keywords: Cloud service provider, Cloud sim, Cloud vendor, Data centre, Edge network, Hybrid clouds, Location identity, Managed service provider, Process segment identity.

I. Introduction

In the service access environment all the client level process can execute the task in the centralized request based operation mode, the significant part of the service access will examines the service utility rate and the interval service transmission time. Hybrid cloud solutions enable the function which can be executes the multiple requests at the same instance. Edge computing will perform the data processing and manipulation operation at the requested end. Hybrid cloud is a kind of cloud computing environment which uses a mix of on-premises control based service access. The private and public clouds needs and costs changing factor to provide the services in a greater flexibility level and finding the number of options to execute the data deployment functions. Any enterprise can deploy the services based on on-premises private cloud to host sensitive or critical workloads and the workloads can be shared and operated by the third party public cloud provider. There are three main reasons to use the hybrid cloud solutions to find the performance rate over the edge network. By applying the security solutions for the cloud operations, the on-premise is still better for network security operations to control the data flow. The enterprise data and systems based operations are migrated to the cloud for the enterprise specific applications.

II. Related Work

As per author Tiago Gama Rodrigues, et.al, "Hybrid method for minimizing service delay in edge cloud computing through VM migration and transmission power control" stated that, in the cloud environment VM migration and monitoring the power control systems users adapted the hybrid mechanism to minimize the rate of service interruption and also minimize the service delay time. This paper has focused only the performance improvement in the edge cloud environment. [1]

Author Abdur Rahman, et.al, "Towards a secure mobile edge computing framework for hajj" stated that, the challenges of providing low latency, high availability of massive resources for the real time location-aware services are the typical process in the cloud service platform. This paper implemented the mobile edge computing framework at the cloud server end by using the fog computing terminals (FCT) at the edge network. Content

aware services are also implemented in the FCT to perform the transactions in a secured manner. [2]

Author, "Liyun Zuo et.al, "A multi objective hybrid cloud resource scheduling method based on deadline and cost constraints", stated that the multi objective decision making model will process the functional optimization component of resource scheduling modelling and reduce the service level cost constraints. The paper has demonstrated all the services in a hybrid cloud platform. [3]

So, from the above papers review, hybrid cloud model was used for the distinct purposes. However, the services can be optimal no approach can specifies the improvement of security value on the hybrid cloud system. The proposed model will use the fuzzy approaches to use the services in an attack free surface at the edge network using the fuzzy logic based implementations.

III. Proposed Work

The edge computing pushes applications, data and computing power services away from centralized points to the logical extremes of the network connectivity. It enables large enterprises to put the correct data in the correct place to support for faster and secure access. A hybrid cloud is a combination of a private cloud combined with the use of public cloud services where one or several touch points exist between the environments. The goal is to combine services and data from a variety of cloud models to create a unified, automated, and well-managed computing environment. Combining the public services with private clouds and the data centre as a hybrid is the new definition of corporate computing. Not all companies that use some public and some private cloud services have a hybrid cloud. Rather, a hybrid cloud is an environment where the private and public services are used together to create value.

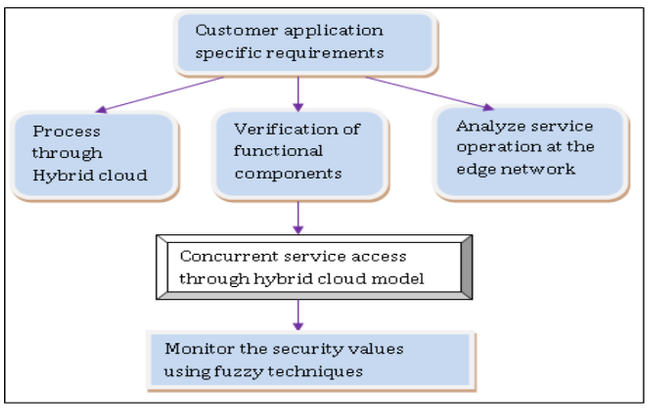


Fig. 1: Illustrating the Functional Process of Proposed Model

If a cloud is processing the applications in a hybrid nature, the following things can be possible which is listed below:

If an enterprise uses the public development platform that sends the secured data over the data centre locations by selecting the appropriate cloud locations.

Resource migration is often happens in the data centre resources whenever there is a request form the client location for improving the services of Saas, PaaS and IaaS generic service applications.

The business based applications need to create the proper designing services, so that all the service based consoles can executes in the single environment.

An above Fig. 1 represents the functional process of the proposed model which will perform the hybrid cloud solutions from distinct user process states. When the user wants to make use of the resources from the underlying hybrid cloud architecture at the edge network environment it explicitly analyze the security credentials for the requested users and improve the security components over the service access.

IV. Implementation Work

The proposed mechanism will operate the hybrid cloud components in the basis of two different types:

- Security analysis in cloud to cloud connectivity
- Cloud to on-premise connectivity

When the user needs to create the security boundaries in their privately stored data value end, then customer are need to use the proper security standards available in the cloud computing environment. Resources are distributed in the cloud to cloud connectivity location (multi clouds) environment, at that instance the CSP need to open the API service access platforms to integrate the services of data management and security tool analysis process. In case of, on-premise based service transactions the enterprises need to create the business solutions for the collaborative service model.

A. Role of Fuzzy Techniques in Hybrid Cloud

Fuzzy logic is a mechanism which performs the distinct computing operations based on the nature of degree of truth for the Boolean logic values in the range between 0 and 1. Fuzzy logic includes the condition derivatives/statements depend on the ambiguity of the problem. User will set the threshold limit to verify the operational sequences which performs the decision making process for the typical problems. Fuzzy logic tool box will optimize the problem/application consequences by using the implication rules. Majorly, fuzzy inference system (FIS) is allowed the user to set the membership function for their own application by defining the rules and adding the variables.

Most of the cases, fuzzy c-means algorithm is used to classify the application type, user access constraints and so forth. C-means algorithm will operate the functional elements under the basic application criterion which satisfies the user service level parameters. The following components are considered in the c-means algorithm which is listed below:

- Application type
- User access privileges
- Fuzzy implication operator
- Type of fuzzy set
- Design goals
- Number of iterations
- Count of cluster groups
- Configuration of cluster data centre
- Type of objective function
- Defining the input and output variable structure through FIS

So, the FCM method can be applied into classifying and clustering the user inputs from the specific problem. Pattern recognition method will be used to minimize the functional risk during the application processing instance. In the hybrid cloud model the user level applications can be processed and iterated in the service access environment which will measure the data within the access limits of data point and objective point values. Hybrid cloud storage will accumulate the contents of sales, business and other process specific data inputs. These inputs are processed in the public cloud environment by considering the additional security privileges.

In edge computing the operational components are used to provide the cloud services by using API and proper network connectivity. The SLA will create the lots of security boundaries for the user services in the cloud environment. Hybrid cloud is managing all the multiple public cloud providers and it is need to analyze the performance efficiency of the specific task which executes on the server-less environment.

V. Results And Discussions

To mitigate the hybrid cloud risks, all the enterprises, organizations and other service specific forums are optimizing the controls with the specific service providers are executing the security control segments over the generic service development platform. It is iterated both in the service provider end and customer end. The hybrid cloud will simulates all the process in the application running environment and it is to be customized with the service level agreement policies. The following simulation set up has been enabled in the security access platform.

Simulator Process Type: cloud sim 3.0 tar.gz

Hypervisor Type: hosted hypervisor

Input Specific Components: user service usage credentials

Application Type: hypervisor segment control

Edge Computing Model: MEC

Platform Used: java JDK 1.7

The multi access edge computing will offers application developers and content providers to use the certain capabilities and the customization in generic service environment. The access specific environment needs to optimize the control specific information for the various virtual segments which integrated on the private cloud and public cloud development model.

Hybrid Cloud Optimization Rate = Edge computing service processed components + service access time+ iteration rate / threshold *100

Resource Access Components Value = Service Automation rate + Security value outcome

Table I: Examining The Resource Access Value From CSP

Cloud Service Type	*Generic User*	*Service Process Segment ID*	*Iterated Performance of Service Access Value (%10)*
SaaS	Frequent user	68.03.1A/E <PID>	8.09
PaaS	Abnormal user	18.045.73.7<PID>	9.62
DaaS	Web blogs user	AE/C.09.4.3<PID>	9.50
NaaS	Group user	EC4.93.82.1<PID>	9.87
CaaS	Iterative User	93.72.21.C<PID>	8.93
IaaS	Managed user	43.94.8.9.B <PID>	9.06

Above Table I illustrates the functional values of the resource access components outcome. The various sets of performance considerations have been implemented in the proposed work. The mechanism is computed the value with the distinct parameter levels.

Table II: Process Of Finding Hybrid Cloud Optimization Outcome

Service Process Segment ID	Iterated Performance Rate (%10)	Threshold limit Value (1 – 5)	Efficiency outcome(%100)
68.03.1A/E <PID>	8.09	4.93	93.92
18.045.73.7<PID>	9.62	3.92	98.27
AE/C.09.4.3<PID>	9.50	4.10	93.84
EC4.93.82.1<PID>	9.87	4.99	99.08
93.72.21.C<PID>	8.93	4.82	92.8
43.94.8.9.B <PID>	9.06	4.61	96.52

Table II will compute the overall functional components value of the hybrid cloud solutions to iterate the process segment ID (PID) along with the threshold limiting set value. This table I and II is cumulatively analyzed the functional components value and also increasing the performance of hybrid clouds in the consumer location.

VI. Experimental Graphs

The various edge network components have been managed and identified with the specific constraint based process outcome. The edge cloud computing operations will specify the functional elements to improve the capability level of experimentation process. The various access specific components are also considered in the proposed approach to evaluate the performance rate of hybrid cloud outcomes. The following graphical illustrations will show the analyzed outcomes of the process of proposed approach.

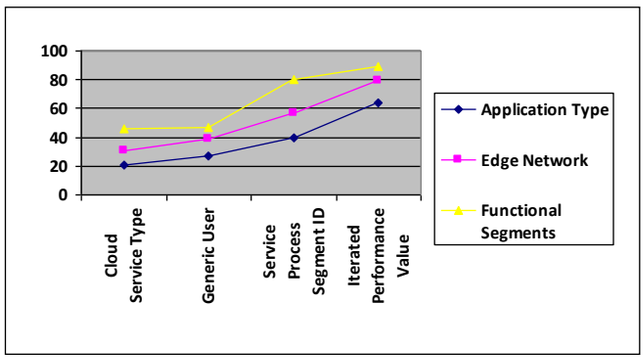
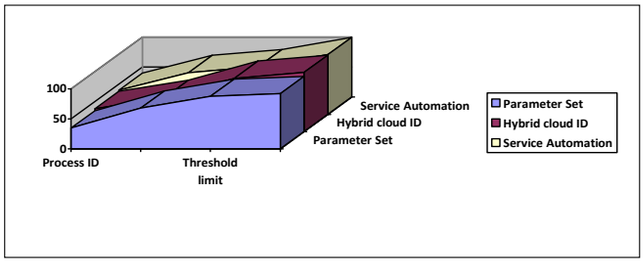


Fig. 2: Access Constraint Set for Edge Network



Above fig. 1 and 2 will depicts the functional graphical outcomes of the increasing hybrid cloud performance value with respect to the parameter set values. The various access specific outcomes are processed in the various intervals along with the threshold limits. The service interruption rate will be calculated and reduce the occurrences of an interruption and also increasing the performance specifications.

VII. Conclusion

The cloud computing environment will facilitates all the operations that can incorporate the functional specifications and the various security parameters are mitigated with the public cloud users. The hybrid cloud will optimize the functional elements which process the services of both public cloud and private cloud. The hybrid cloud solutions are increased in the edge network and optimize the performance in the service consumption and service interruption need to be reduced in the cloud platform.

VIII. Future Enhancement

Edge computing is the latest technology will brings the lots of solutions to increase the functional access limits with the service specifications and also perhaps the security solutions over the security platform. The technology can be applied into the domains of deep learning, visual computing and video enhancement in the future cases.

References

1. T. G. Rodrigues, and K. Suto, “Hybrid method for minimizing service delay in edge cloud computing through VM migration and transmission power control,” *IEEE Transactions on Computers*, vol. 66, no. 5, pp. 810-819, 2017.
2. A. Rahman, and E. Hassanain, “Towards a secure mobile edge computing framework for Hajj,” *IEEE Access*, vol. 5, pp. 11768-11781, 2017.

3. Z. Yan, and J. Xue, "Prius: Hybrid edge cloud and client adaptation for HTTP adaptive streaming in cellular networks," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 1, pp. 209-222, 2017.
4. K. Bhaskar, R. Jayashree, R. Sathiyavathi, L. M. Gladence, and V. M. Anu, "A novel approach for securing data de-duplication methodology in hybrid cloud storage," *International Conference on Innovations in Information Embedded and Communication Systems*, pp. 1-5, 2017.
5. L. Zuo, and L. Shu, "A multi-objective hybrid cloud resource scheduling method based on deadline and cost constraints", *IEEE Access*, vol. 5, pp. 22067-22080, 2017.
6. R. Garcia, "Federated identity hybrid cloud security considerations supporting first responders," *IEEE Conference on Dependable and Secure Computing,* pp. 326-333, 2017
7. C. Gopinaath, and A. Kiruthika, "A server side encryption for cloud storage with federation sharing in hybrid cloud environment," *International Conference on Technical Advancements in Computers and Communications,* pp. 128-130, 2017.
8. C. Hongbing, and R. Chunming, "Secure big data storage and sharing scheme for cloud tenants," *IEEE Transactions on Communication Systems,* vol. 12, no. 6, 2015.
9. J. Baek, and Q. H. Vu, "A secure cloud computing based framework for big data information management of smart grid," *IEEE Transactions on Cloud Computing,* vol 3, no. 2, 2015.
10. N. V. Juliadotter, and K. K. R. Choo, "Cloud attack and risk assessment taxonomy," *IEEE Transactions on Cloud Computing*, vol. 2, no. 1, pp. 14-20, January-February 2015.
11. Y. Xuanxia, H. Liu, H. Ning, L. T. Yang, and Y. Xiang, "Anonymous credential-based access control scheme for clouds," *IEEE Transactions on Cloud Computing,* vol. 2, no. 4, pp. 34-43, 2015.
12. H. Liu, and H. Ning, "Shared authority based privacy-preserving authentication protocol in cloud computing," *IEEE Transactions on Systems*, vol. 26, no. 1, pp. 241-251, 2015.