INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 5, Issue 2)***
Available online at: www.ijariit.com

# Augmentation of information management protection in hybrid clouds

*Dr. R. Poorvadevi*
*rpoorvadevi@kanchiuniv.ac.in*
*Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya University,*
*Kanchipuram, Tamil Nadu*

## ABSTRACT

***As the growing technology of cloud, tremendous information is generated every day from multiple sources. Information is receiving from the distinct data centre as a collaborated service nature of computing technology. Hybrid cloud model will hold the business critical content securely and on-premises control enables the process of consumer grade level alternative solutions. However, there will be a process specific security controls in the content-specific environments, it is important to manage all generic type of information and its sources in hybrid cloud access platform. Hybrid cloud platform deals with various business insights, which increases the volume of cloud systems. Any private and public users can request for cloud services and use it as a model of on-demand services. It is necessary to monitor and regulate the security systems for controlling access from generating a large amount of data. So, the proposed system will bring the solution for a secured level of information management in a hybrid cloud service model.***

***Keywords—*** *Cloud Vendor, Hybrid Cloud, Information Process, Service Level Agreement, Identity and Access Management, Cloud Service Provider, Service Provisioning*

## 1. INTRODUCTION

In the cloud computing era, identity and access management (IAM) play a vital role for evaluating the cloud service access solutions. The cloud service provider will offer plenty of cloud automation services to its requested user. Though, the user can avail the service of security-as-a-service from the cloud server still there is a security issue among the hybrid cloud deployment model.

The business agility process can infer the availability of service based content and its resourcefulness is to be monitored by the cloud service provider. Any enterprises that will render the security solutions to the end user by analyzing the service and access level information. Innovative based technological solutions need to provide assurance for information governance

## 2. LITERATURE SURVEY

As per an author Asma Islam Swapna et.al, "Performance evaluation of fuzzy integrated firewall model for hybrid cloud based on packet utilization". This paper stated that for the hybrid cloud model based packet utilization evaluated the fuzzy integrated firewall which emphasizes the process of determining the performance level of hybrid cloud operations with the fuzzy-based integration services. [1]

Author Uthpala premarathne et.al, "Hybrid cryptographic access control for cloud-based EHR systems". This paper has implemented the access control privileges for an enterprise system with the help of cryptographic-based functional components in a hybrid cloud platform. [2]

Author Mayur U. Kolhatkar et.al, "A review on hybrid cloud approach for sharing health information and management". This paper has reviewed the concept of health information sharing and management in hybrid cloud platform which perhaps the adoption of hybrid cloud services solutions in the healthcare systems. [3]

Shigeaki Tanimoto et.al, "A study of data management in hybrid cloud configuration". This paper proposed the concept of handling data management in hybrid cloud configuration and the study report shows that heterogeneous data management and data acquisition process are reviewed. [4]

 

From the literature survey reviews, information management has been adapted in the hybrid cloud model and there is no perfect evidence for the security solutions among the cloud users. So, the proposed model will bring the solution for securing information management process under the hybrid cloud infrastructure.

## 3. PROPOSED WORK

The hybrid cloud management model will provide the infrastructure for private and public cloud services will run the applications, and analyzing the security patterns and also managing of data across the cloud servers. Hybrid cloud management strategy will clearly analyze the user workloads on the public and private cloud platforms to enable the functional operations of customized applications. The following parameters were used to consider in the proposed work which is listed below:

- Nature of user application
- Level of interaction with the end users
- Managing heterogeneous data
- Network handling
- Security patterns values
- Performance up gradation

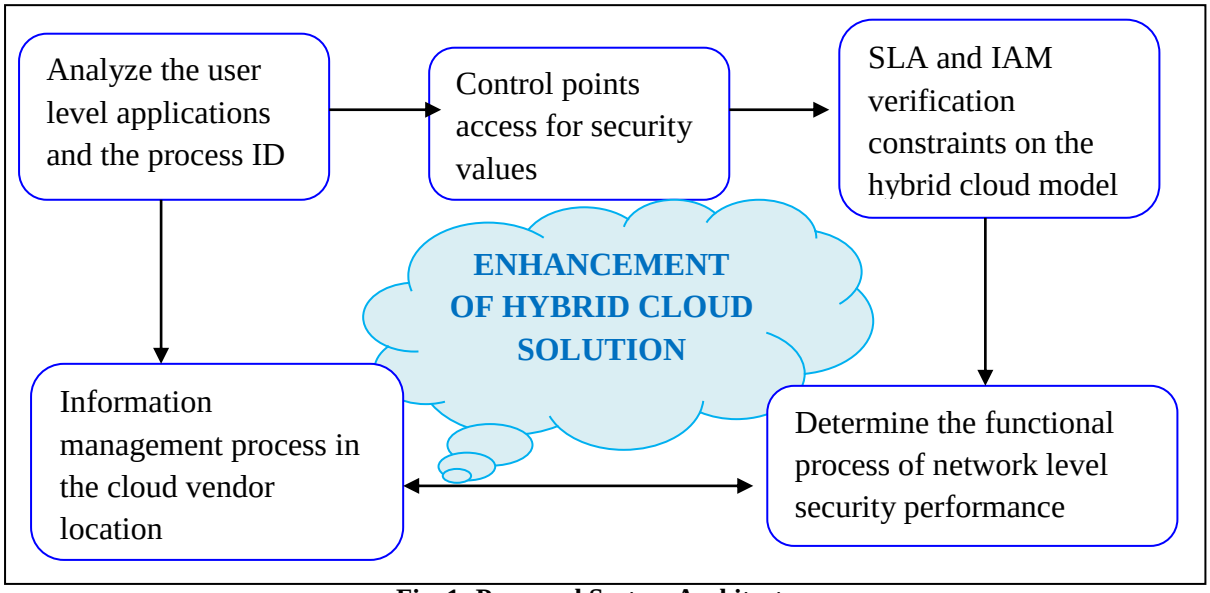


**Fig. 1: Proposed System Architecture**

An above system architecture figure 1 illustrates the process iterations in the hybrid cloud model which facilitates the workloads optimizing and evaluating the security patterns values of the simulator and the infrastructure level security of cloud service provider. It will also iterate the performance of information sharing during the client level service processing time.

## 4. IMPLEMENTATION WORK

Critical security applications were clearly noted and processed on the environment of cloud user cluster groups in order to perform an accurate decision-making process. This process will find out the resources that are spent for managing workloads can be used to value the business level applications. Hybrid cloud synchronizes the re-evaluation of security parameters. The security parameters will include the following:

- User service provisioning ID
- Process segment values
- User application requirements
- Proactive security managing values
- Identities of people, devices, and server level information
- Configuring the information processor set-up
- Encrypting the information with the suitable key pair values

All the generic processes are iterated with the customers level requirements need to be processed on the server level validation to leverage the mechanism values of security and its performance verification process.

### 4.1 Process of security and Performance Finding

This is the initial process function to elaborate the functional process of finding the user level workloads and the information need to be encrypted with the network identical values on the client service access platforms. Lots of security functions are simulated with the copies of information exchanges, managing of I/O process, resource utilization rate and the generic functional components of performance and monitoring tools.

### 4.2 Security Level Policy Management

Governance requires that policies are written and enforced, and this enforcement needs to be understood by those who are managing the hybrid cloud so that they do not conflict or otherwise get in the way of operations. This level of security operations

 

was identified with the functional process of segmenting the security key codes with the assigned security values that can be operated on the client specific applications to validate the authorized functional elements.

## 5. EXPERIMENTAL GRAPHS AND RESULTS DISCUSSIONS

In the hybrid cloud model proposing the solution form information management is the trivial process in service access environment. All the elements can be operated in the single authenticity parameters to validate the client level process by maintaining and accessing through API's and other security relevant resources. Security values are built with the components of storage managing, networking policies, networking, and service provisioning interfaces to avoid the complex functions. There are tools that can manage the cloud services using a single interface to translate what something means on one cloud versus another cloud. All the SLA's constraints are compromised with both end users and cloud servers.

**Table: 1 Information management processed outcomes**

| Service provisioning ID | Information Access Zone Status | Security constraints with policy constraints | Hybrid Cloud model security Efficiency (%100) |
|---|---|---|---|
| ID:09:A65:97:10 | Processed | Matched | 89.03 |
| ID:92:872:CF:S5:92 | Iterated | Matched | 94.6 |
| ID:16:57:AE:BC:187 | Segmented | Matched | 98.8 |
| ID:93:62:98:41:CF:53 | Processed | Matched | 98.73 |
| ID:09:BL:64:03:82 | Verified | Accessed | 97.19 |

Many charged with hybrid cloud management often focus too much on the management tools that are available. These tools cover areas such as API management, resource management, cloud management platforms, performance management, DevOps management, security management, network management, native platform management, and another set of security tools. Table 1 will illustrate the process level information in order to find the resources with the specific access level security components on the hybrid cloud model.

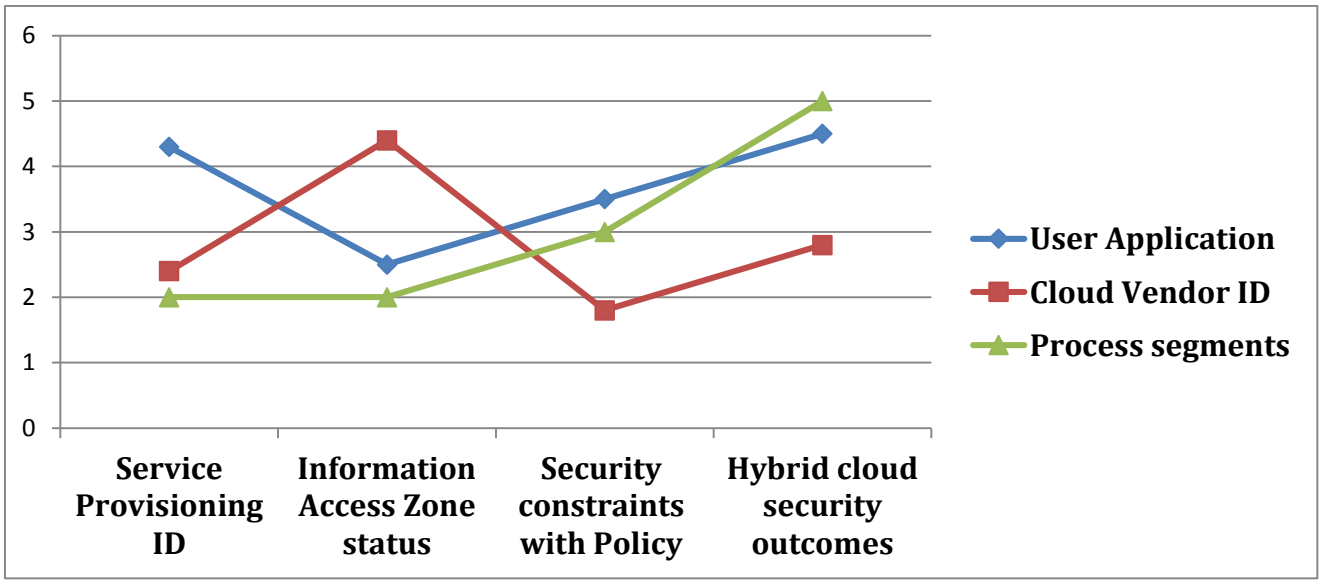


**Fig. 2: Experimental result analysis outcome**

The above figure performed the operational values of all generic level application are need to be identified and processed on the client level security platforms. To mitigate the security level policies all the functional components were examined in the user-specific process.

## 6. CONCLUSION

From the implementation work and results it is showing that all the processes are compared with the analytical parameters with the security level constraints in order to facilitate the secure level of information management need to be done in the client service access environment.

## 7. REFERENCES

[1] Shigeaki Tanimoto; Yorihiro Sakurada ; Yosiaki Seki et.al,"A Study of Data Management in Hybrid Cloud Configuration",14th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, Year: 2013, Pages: 381 - 386

[2] Mayur U. Kolhatkar; Veena A. Gulhane,"A review on hybrid cloud approach for sharing health information and management", 2017 International Conference on Inventive Systems and Control (ICISC), 2017, Page(s):1 - 4

[3] Asma Islam Swapna; Ziaur Rahman; Md. Habibur Rahman; Md. Akramuzzaman, "Performance evaluation of fuzzy integrated firewall model for hybrid cloud based on packet utilization", First IEEE International Conference on Computer Communication and the Internet (ICCCI), Year: 2016, Pages: 253 - 256

 

[4] Uthpala Premarathne; Alsharif Abuadbba ; Abdulatif Alabdulatif ; Ibrahim Khalil ; Zahir Tari ; Albert Zomaya ; Rajkumar Buyya, "Hybrid Cryptographic Access Control for Cloud-Based EHR Systems", IEEE Cloud Computing, Year: 2016, Volume: Issue: 4, Pages: 58 - 64

[5] Yuya Jeremy Ong; Mu Qiao ; Ramani Routray ; Roger Raphael, "Context-Aware Data Loss Prevention for Cloud Storage Services", IEEE 10th International Conference on Cloud Computing (CLOUD), Year: 2017, Pages: 399 - 406

[6] Bingwei Liu; Yu Chen ; Ari Hadiks ; Erik Blasch ; Alex Aved ; Dan Shen et.al, "Information fusion in a cloud computing era: A systems-level perspective", IEEE Journal on Aerospace and Electronic Systems Magazine, Year: 2014, Volume: 29, Issue: 10, Pages: 16 - 24

[7] Vladimir Tosic; Hiroshi Wada ; Adnene Guabtni ; Kevin Lee ; Anna Liu, "Management towards reducing cloud usage costs", 7th Latin American Network Operations and Management Symposium, Year: 2011, Pages: 1 - 1

[8] G ina hung Wang ; Kuochen Wang,"An efficient hybrid P2P MMOG cloud architecture for dynamic load management", The International Conference on Information Network 2012, Pages: 199 - 204

 