https://dx.doi.org/10.22161/ijaers.4.3.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

A Study on Various Security Aspects in Cloud Policy Oriented Architecture

Sonia[1], Kirti Bhatia[2]

[1]Department of CSE, M.Tech. (student) Sat Kabir Institute of Technology and Management, Bahadurgarh, India
[2]HOD, Department of CSE, Sat Kabir Institute of Technology and Management, Bahadurgarh, India

Abstract— *Security is the major requirement for data environment. A cloud system provides the data repository and services in public domain so that it suffers from various security specific threats. The presented work is here defined to analyze the policy driven architecture for cloud system as well as identify the associated criticalities. The work also cover the process stage of this security driven architecture so that the interconnection model can be explored. The system is also defined the secure system integration under the service aspect specification. The work is defined as an improvement to the security system architecture under policy driven specifications.*

Keywords— Policy Driven, Secure, Architecture, Cloud System, File System.

I. INTRODUCTION

A cloud environment actually provides the integration to the virtual aspects in the cloud system with specification of data distribution, service distribution and platform distribution. These shared systems improve the system capabilities so that the better utilization of available system resources will be done. These kind of systems are available in public domain with private constraints. The constraints are defined in terms of various rules defined to provide system level access and service level integration so that the system improvement and the aspect analysis can be obtained. The shared system is here defined under the environmental constraints. The resource distribution and service specifications are provided at different levels of distribution sothat the robust and improved integrity system will be obtained. Here figure1 is showing the interconnection model for cloud system. The model is showing the physical characteristics driven architecture. The cloud system is here defined as the global cloud environment. The interconnection system is here defined with specification of interconnection devices. These devices include the switch inclusion and routers. The switches where provided the low level platform switching if the client is not capable to handle the cloud system content. The platform level independence is provided the switches. The routers are defined to integrate the global environment with client system. This global environment is defined to provide the distribution localized information storage among available multiple clouds. The selection of this storage cloud depends on multiple parameters such as client localization, load, scheduling mechanism etc.

As the cloud system is configured, it is defined by multiple number of cloud servers integrated in a global environment. Each of the server is defined with relative constraints such as accessibility, security restriction, resource availability vector, connectivity domain, restricted access constraints etc. These cloud servers are the physical entities defined with the memory, processing system and the device integration.

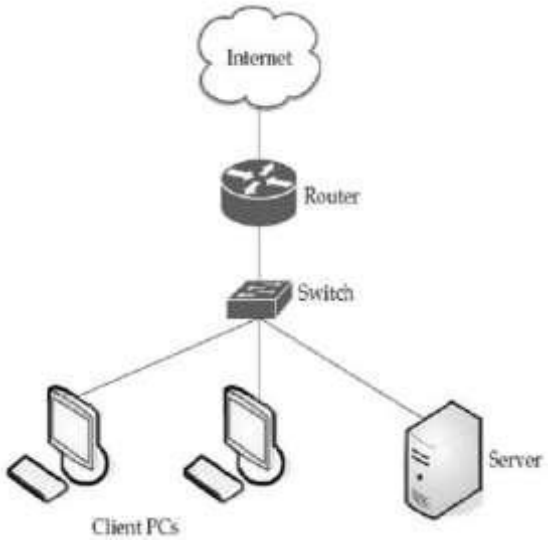

Fig.1: Cloud Service Interaction System

The physical parameters of the cloud system are not available to the client environment but some of the intermediate layer can access these characteristics to device the cloud server performance and reliability vector.

The cloud system is further divided in multiple virtual machines so that the maximum utilization of cloud server capabilities will be done. The virtual machines are divided to achieve the work load over the cloud system. This work load distribution is achieved in terms of number of requests processed by the system, service load, security requirements, location of server etc. The

https://dx.doi.org/10.22161/ijaers.4.3.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

processing architecture of cloud system is shown in figure 2.

The figure is showing the data driven, storage driven secure system architecture. The main model is divided in two sub blocks. The first block is here defined to achieve the storage level and data level security and the second block is defined to process the user level data access and security.

A) Layer I

The first layer of this model is described as the high security or data model that defines the physical constraints related to the system. These constraints includes the cluster generation at the server end and the data formation based under the specification of location driven clustering, data driven clustering and user specific clustering. This clustering process is performed on the inner most layer of the cloud system. Once the storage system is configured, the next work is to provide the interaction between this data system and the cloud servers. The data blocker is defined between the data architectural view and the cloud servers to provide the effective system allocation. This allocation process is here defined under the constraints and the configuration management. The cloud server performance, requirement and the security constraints are here identified by the brocker to allocate the clusters to the cloud server. A cloud server can allocate one or more clusters based on the specification and the relative constraints.

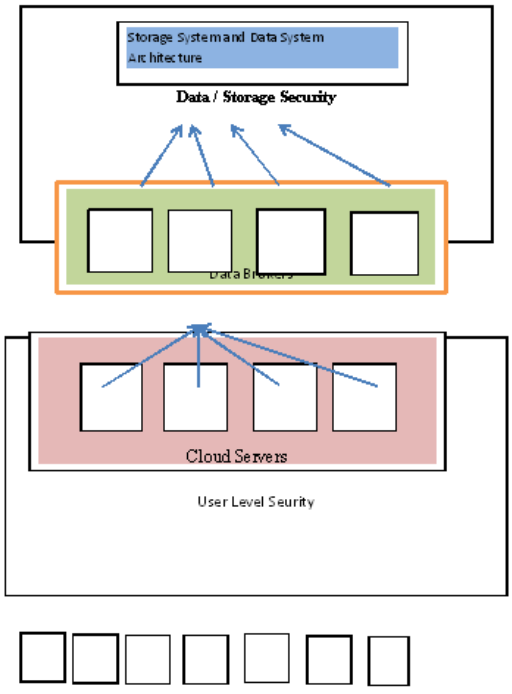

Fig.2: Data Access Architecture

B) Layer II

This layer is defined as the second stage model applied between the cloud server system and the client integration. This integration process is defined with specification of multiple clients. Each client is defined in two main categories called public user or the licensed users. The public users are the free users and of low priority whereas the licensed users are the application specific or service specific users. Once the multiple requests are applied on server with specification of requirement constraints. The intermediate model accept these request and perform the request analysis. The analysis is performed on the request parameters and security requirements. Based on this analysis, the allocation to the particular cloud server is done.

In this paper, a security driven policy architecture is defined in which the data and the services are available to the cloud system. The paper has explored the cloud system data model and the process integration under policy driven architecture. In this section, the cloud system architecture is presented as the global view as well as detailed data view. The section has divided the data modeling on cloud system in two main stages. In first stage, the physical characteristic the storage space allocation to cloud servers is described and in second layer, the client driven mapping is done. In section II, some of the work defined by earlier researchers is described. In section III, the policy driven model along with characteristics exploration is described. In section IV, the conclusion obtained from the work is presented.

II. EXISTING WORK

Lot of work is already presented by different cloud servers to explore the cloud system architecture under different constraints. These architecture and relative improvements are suggested by many researchers. In this section, some of the contribution of earlier researchers is discussed. Ching-Nung Yang[1] has presented a data driven architecture in hadoop environment. The defined system is able to improve the service driven architecture in haddoop system along with the storage policy specification. Author also presented the key based secure system to explore the system resources and the authentication to the system. The system modeling is here done to achieve the symmetric, bivariate information processing in distributed environment. Author explored the service policies and defined a service driven mechanism to improve the cloud service distribution in public environment with private constraints integration. J. McDermott [2] presented an application effective cloud environment for military application. Author defined a work on infrastructure driven analysis so that the processing in virtual environment will be done. Author defined the secure system layer specification for authentication to the system. Author presented a kernel

https://dx.doi.org/10.22161/ijaers.4.3.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

driven mechanism to perform the systematic security checks for users in cloud system environment. Jonathan A.P. Marpaung [3] presented a work in hadoop environment to define a security architecture for cloud system. Author defined a cloud system based analytical study on the secure environment and its future mapping with key driven constraint. Auhtor defined the work on the service integration under security constraints so that the scaled system development will be obtained.

Piotr K. Tysowski [4] presented a work on scalable Hadoop environment with specification of application level constraints. Author defined a Hadoop environment so that policy driven constraints are described. Author defined the specification of key management scheme so that the secure application constraints are described. Author defined a coordination over the server and the system users so that the information tracking will done in secure way. Chang-Ji WANG [5] defined a work on encryption driven processing for cipher text generation and processing under cryptographic algorithmic approach. Author defined a grained data processing with shared decentralized system to achieve the access control so that the policy driven architecture will be formed. Author provided the size specification and data sharing capabilities in secure system so that the storage and structural aspects of cloud system are described and improved. Author defined the hadoop based storage system with integrated key exchange mechanism using Diffie Hellman Approach. Dexian Chang [6] provided a work on relationship analysis in virtual cloud environment with specification of user domain. Author defined a trust mechanism with migration constraints so that the reliable system composition will be obtained. Author defined the inter domain communication in virtual environment so that the server level integration for the cloud system will be improved.

M.Venkatesh [7] has provided a secure data storage system under public auditability so that the system integration and feature extraction with data support system will be obtained. Author defined the secure remote communication with specification of data utilization aspects. Author defined a RSA inclusive security system to achieve the public information auditing so that the security over the system will be improved. Author defined the time domain specific constraints so that the improved system integration will be achieved. Author provided the work under secure system constraints so that the derivation to the work will be done under multiple information constraints and provides the system improved under critical information aspects. Sahil Madaan[8] has provided a secure system for hadoop system environment. Author improved the root oriented security in cloud system in distributed policy driven environment. Author analyze the cloud system under identity analysis so that the secure system behavior will be achieved. Author integrated the third party in the system for improving the system robustness and security. Tamal Kanti Chakraborty [9] has provided the cloud system integration and security under resolvement of various associated issues. Author provided a long term solution for cryptographic and authenticated problems. Author provided the secure way for information collection and problem rectification so that the domain specific communication over the system will be performed.

Vasyl Ustimenko [10] provided a work on cloud system aspect formation and homomorphic encryption process applied with muti variate key specification. Author improved the system by integrating the quantum cryptography. Christian Schridde[11]presented an infrastructure driven process model for secure cloud system composition under data integration and data modeling with constraint specification. The trust vector is here performed to improve the system integration in security domain. Yingjie Xia[12] has provided a work on ECC based secure system to improve the communication constraints under protocol specification. Author defined the policy driven communication with security specification.

III. SECURITY INCLUSIVE POLICY DRIVEN CLOUD MODEL

In this section, the cloud security distribution environment is defined to provide the effective service distribution. In this section, the policy model aspects and the functioning are described in detail. The section includes the effective constraint specification with rule specification under associated constraints. As a policy driven architecture is defined, the model includes the integrated with some integrated security constraints. These policy specification are defined in figure 3. The figure shows that the complete model is divided in four main phases to setup different process constraints.

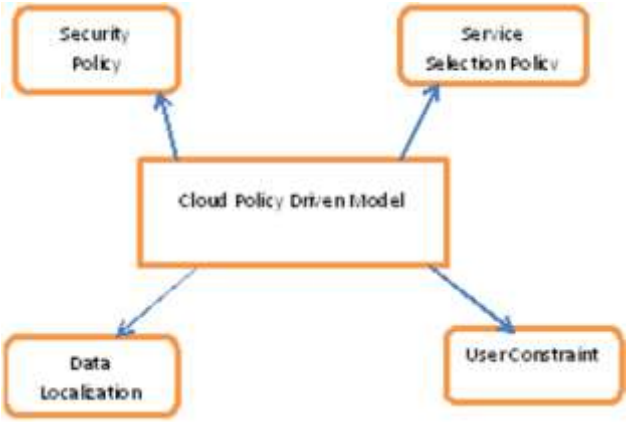

Fig.3: Policies Under Scheduling Consideration

https://dx.doi.org/10.22161/ijaers.4.3.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

A) Security Policy

The security is the foremost constraint and requirement for cloud system model. This policy model is defined at different level to identify th`e type of security required in the system. These all security constraints or types include data driven security, user level security, communication level security. The security constraints are applied between two stages of the cloud system model. It can be applied between the hardware and the cloud server to achieve the data driven security at low level. In second security model, the security integration is defined as the middle layer between the clients and the cloud server. In this layer, the cloud system authentication, communication level security and data driven security can be applied. This security policy is defined to achieve the secure communication. The policy is able to provide the separation of available services based on the secure component availability and requirements.

B) Service Selection Policy

This policy rule basically defines as the middle layer architecture provides the effective service selection. This service selection is based on multiple parameters. These parameters include the availability of cloud service, reliability vector, response time etc. The service driven policy analysis is here performed to provide the analysis between the requirements and availability. This parameter specification s here defined under multiple constraints and parameters. These all associated constraints are shown in figure 4.

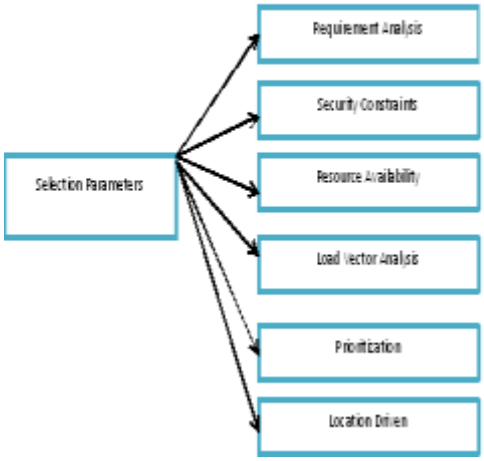

Fig.4 : Service Selection Policy

C) Data Localization Policy

The localization policy actually defines the availability of the requested information on the particular cloud server as well as the way of availing the information on service request. The localization policy defines the process applied on specialized server under the integration of data base server and services. The localization is here defined three main parameters called transparency vector, scalability and access robustness. The process driven mechanism is here defined to achieve the data modeling so that the attribute specification analysis on the request is done. Based on the request feature analysis, the physical location of the data or request elements can be obtained. The utilization server specification along with domain specification is done under the location boundation and the user specification. The user constraints are defined as the selection process under the security and the requirement constraints. The location driven parameter are shown in figure 5.

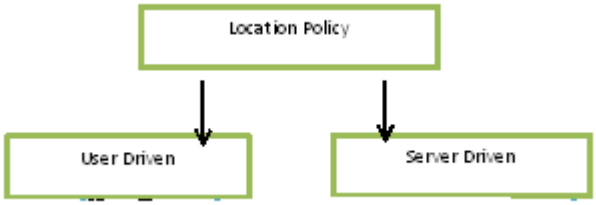

Fig.5: Location Driven Policy

The requirement constraints are here defined under adaptive feature constraints and load vectors. These vectors include the adaptive information assignment to various cloud system with specification of requirement and availability constraints.

D) User Policy The user is the actual element in the process policy model that actually perform the information request on cloud server. The request performed by a user is processed by middle layer architecture and processed on cloud server to extract the information. This stage includes the server driven processing, constraints satisfaction, security constraint specification. The process processing modeling is here defined to identify the service driven architecture. The user specification and constraints consider in this model are shown in figure 6

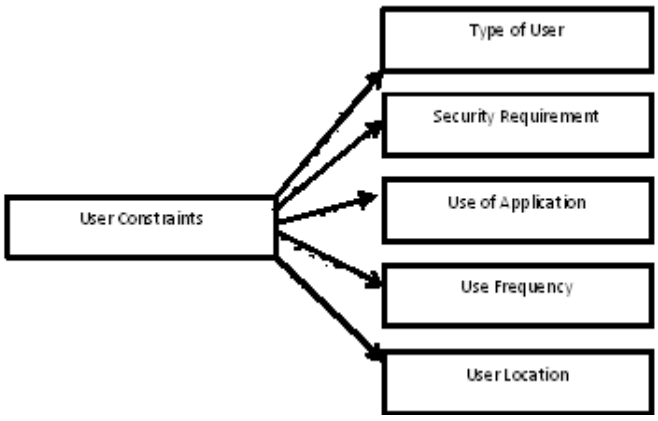

Fig.6: User Constraints

https://dx.doi.org/10.22161/ijaers.4.3.30 *ISSN: 2349-6495(P) | 2456-1908(O)*

Once these all constraints are processed, the intermediate layer identify the appropriate cloud system that can fulfill the request of user.

IV. CONCLUSION

In this paper, the complete cloud system model is described under the security and policy driven mechanism. This model is here defined with four main stages and policies. These policies include user level policy, data localization policy, security policy and service selection policy. Based on these all constraints and stages the user request can be processed on cloud system and the service availability in secure way can be obtained.

REFERENCES

[1] Vikki Tang," A Framework for Reducing Instruction Scheduling Overhead in Dynamic Compilers".

[2] Lichen Weng," Scheduling Optimization in Multicore Multithreaded MicroDistributed Clouds through Dynamic Modeling", CF'13, May 14–16, 2013, Ischia, Italy. ACM 978-1-4503-2053-5

[3] Hsiang-Yun Cheng," An Analytical Model to Exploit Memory Task Scheduling", INTERACT-14, March 13, 2010, Pittsburgh, PA, USA ACM 978-1-60558-921-3/10/03

[4] Vishakha Gupta," Kinship: Efficient Resource Management for Performance and Functionally Asymmetric Platforms", CF'13, May 14–16, 2013, Ischia, Italy. ACM 978-1-4503-2053-5

[5] Morris A. Jette," Performance Characteristics of Gang Scheduling in Multiprogrammed Environments", 1997 ACM 0-89791-985-8/97/0011

[6] Minyoung Kim," Design Space Exploration of Real-time Multi-media MPSoCs with Heterogeneous Scheduling Policies", CODES+ISSS'06, October 22–25, 2006, Seoul, Korea. ACM 1-59593-370-0/06/0010

[7] Jonathan A. Winter," Scalable Thread Scheduling and Global Power Management for Heterogeneous Many-Core Architectures", PACT'10, September 11–15, 2010, Vienna, Austria. ACM 978-1-4503-0178-7/10/09

[8] Rony Ghattas," Energy Management for Commodity Short-Bit-Width Microcontrollers", CASES'05, September 24–27, 2005, San Francisco, California, USA. ACM 1-59593-149-X/05/0009

[9] Andrei Terechko," Cluster Assignment of Global Values for Clustered VLIW Distributed Clouds", CASES'03, Oct. 30 – Nov. 1, 2003, San Jose, California, USA. ACM 1-58113-676-5/03/0010

[10] Andrew Riffel," Mio: Fast Multipass Partitioning via Priority-Based Instruction Scheduling".

[11] Hiroshi Sasaki,"Energy-Efficient Dynamic Instruction Scheduling Logic through Instruction Grouping", ISLPED'06, October 4–6, 2006, Tegernsee, Germany. ACM 1-59593-462-6/06/0010

[12] Flavius Gruian," Hard Real-Time Scheduling for Low-Energy Using Stochastic Data and DVS Distributed Clouds", ISLPED'01, August 6-7, 2001, Huntington Beach, California, USA. ACM 1-58113-371-5/01/0008

[13] Martin Schoeberl," Architecture for Object-Oriented Programming Languages", JTRES '07 September 26-28, 2007 Vienna, Austria ACM 978-59593-813-8/07/09

[14] Jared Stark," On Pipelining Dynamic Instruction Scheduling Logic", 0-7695-0924-X/2000© 2000 IEEE.