IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 01-06

Big Data Analysis for Associated Cloud Service using Parallel Trust Computing: A Survey.

Monika Gedam.[1] BharatiAinapure. [2]
[1] *(Student, M.Tech. Computer Science and Engineering (Data Science and Analysis)MIT- WPU, pune)*
[2]*(Professor,Computer Science and Engineering, MIT- WPU, pune)*

Abstract: *This survey paper presents on-going research on the development of Intercloud Architecture Framework (ICAF) that examines the drawbacks of multi-provider multi-domain miscellaneous cloud that are based on infrastructure services and applications integration and interoperability.*
Cloud services model that merge frequently used cloud service models, like IaaS, PaaS, SaaS, in one multilayer model with corresponding inter-layer interfaces.Intercloud Controlling and Management Plane are based on applications interaction that supports cloud.To accessing trustworthy cloud services is the main task for any cloud computing platform.
Keywords: *Intercloud, Cloud Computing, Cloud Computing Security, Trust Computing, Big Data Analysis.*

I. Introduction

Cloud technologies bring applications and infrastructure services mobility and physical/hardware platform independence to the present distributed computing and networking applications.

Intercloud:-
The networks known as the "Internet"; in a world of Cloud Computing, content, storage and computing is ubiquitous and interoperable in a network of Clouds known as the "Intercloud".

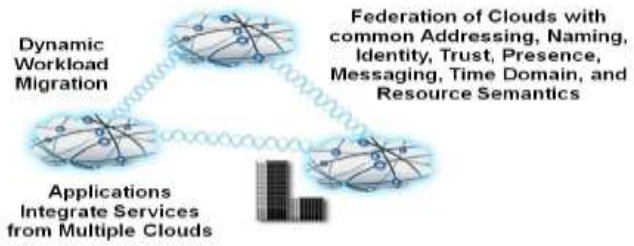

Figure: -The Intercloud Vision [1]

Individual Intercloud is capable for communicating with each other, as clients, through the server environment which is hosted by Intercloud Roots and Intercloud Exchanges.
Complementary components of the proposed Intercloud Architecture:

(1) Multilayer Cloud Services Model (CSM) - is commonly used for vertical cloud services , both relations between cloud service models (such as IaaS, PaaS, SaaS) and other required functional layers and components of the general cloud-based services infrastructure are define by integration and compatibility respectively.
The three vertical planes infrastructures can define following functionality of CSM;

- Control and Management Plane.
- Operations Support System.
- Security Infrastructure.

(2) Intercloud Control and Management Plane (ICCMP) - it is usedfor inter-cloud applications and infrastructure control. The management also includes inter-applications signaling, synchronization and session management, configuration,monitoring, run time infrastructure optimization includingVM migration, resources scaling, and jobs/objects routing.
The ICCMP Interfaces support some functionality that is listed below;

- Inter-/cross-layer control and signaling.
- Monitoring.

- Location service.
- Topology aware infrastructure management.
- Configuration and protocols management.

(3) Intercloud Federation Framework (ICFF) - It allowindependent clouds and its related infrastructure componentsfederation to manage independently the cloud basedinfrastructure components belonging to different cloudproviders and/or administrative domains. It should support to the level of services, business applications,semantics, and namespaces or assuming necessary gateway.

Table: -Operations and functionalities of Intercloud Federation Framework (ICFF)

Federated inter-cloud infrastructure supports following operations	**The ICFF Interfaces support the following functionalities**
Trust and service brokers	Publishing
Service Registry	Naming, Addressing and Translation (if/as needed)
Identity provider (IdP)	Attributes management
Trust manager/router	Discovery
Service Discovery	Trust/key management

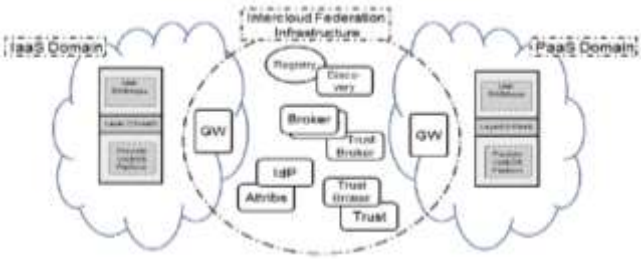

Figure. ICFF components[3] . (

4) Intercloud Operation Framework (ICOF)- Itincludes functionalities that support multi-providerinfrastructure operation, including business workflow, SLAmanagement, and accounting. ICOF also defines the basic roles,actors and their relations in sense of resources operation,management and ownership. ICOF requires the supportand interacts with both ICCMP and ICFF respectively.

Main functional components	**ICOF interfaces should support the following functionalities**
Service Broker	Service Provisioning
Service Registry	Deployment
Cloud Service Provider, Cloud Operator	Decommissioning (or Termination)
Cloud (physical) Resource provider, Cloud Carrier	SLA management and negotiation
-	Services Lifecycle and metadata management

Table: - Functional components and functionalities of Intercloud Operation Framework (ICOF)

Monitoring Agent
Management

When a cloud provider registers its resources in the cloud broker, the registered resource demands to download a monitoring agent and bind this monitoring agent with its IP. If a computing task is distributed to this resource, the monitoring agent will be activated and then begin its monitoring task.

Trust Computing Based On Big Data Analysis

To accelerate pre-processing andperceiving the trust behavior indicators, two types of software agents are exploited.

1) SMAs (security monitoring agents) : -

SMAs are responsible for collecting security-related data, such as the authentication type, the authorization type, the self-security competence and the number of malicious access.

2) QMAs (QoS monitoring agents): -

QMAs responsible for collecting and pre-processing QoS-related information, most of which are the indirect trust indicators, and need calculation and pre-processing based on a given time period.

In this work, we will present an updated survey on recent development and focus on the future research and development trends in Big Data Analysis for Associated Cloud Service field. We have initially discussed Introduction in section I, then secondly the literature review in Section II. Section III, we discuss the different technologies that are used for big data analysis for cloud service field. Section IV contains advantages and finally, concluding remark will be given in Section V.

II. Literature Review

[1] David Bernstein et al Intercloud Security Considerations Cloud computing is a new design example for large, distributed datacenters. In cloud computing users can store their data using cloud infrastructure and even they can access the applications like email, search, and social networks, Service providers offer These all services.

Advantage: -

The key benefit of the system is its deterministic behavior and the fair balancing of load among the peers.

[10]Yuri Demchenko et al introduced a system that represents the research work for developing the Intercloud Architecture Framework (ICAF). This ICAF system defines four corresponding components of Intercloud integration and interoperability: multilayer Cloud Services Model; Intercloud Control and Management Plane; Intercloud Federation Framework, and Intercloud Operation Framework. The architecture provides the model for developing Intercloud middleware for making possible clouds interoperability and integration.

Advantage:-

Developing Intercloud middleware and facilitate clouds interoperability and integration.

[7]Hamid MohammadiFard et al the system will propose a pricing model and truthful mechanism for dynamic scheduling of a single task in commercial multi-Cloud environment. The system will schedule the scientific workflows with respect to optimization of two objectives, makespan and monetary cost, and proved the truthfulness of the mechanism theoretically. The proposed system used the (BOSS) Bi-Objective Scheduling Strategy for dynamic scheduling.

Advantage:-

The goal is to satisfy an application deadline by extending the local computational capacity with Cloud resources.

[8]Xiaoyong Li et al this paper present a service operator-aware trust scheme (SOTS) for resource matchmaking across multiple clouds. According to multi-dimensional resource the operator, model trust andevaluate the process. The multi-attribute decision-making, and develop an adaptive trust evaluation approach based on information entropy theory. This approach can overcome the limitations of traditional trust schemes, and the trusted operators are weighted manually or subjectively.

Advantage:-

The middleware trust management framework is used for reducing the user burden and improving system dependability.

[3]ShirleiAparecida de Chaves et al This work describe an architecture for and implementation of a private cloud monitoring system. This is quite high-level architecture and it contains three layers: an Infrastructure layer, an Integration layer and a View layer respectively. The implementation is modular in design and consists of different components that are mainly focused on the integration layer of the architecture. Recently, it is compatible with Eucalyptus as a IaaS implementation therefore, it is mentioned that it could be extended to work with alternative IaaS implementations in the future. It appears to rely quite heavily on Nagios for its monitoring functionality.

Advantage:-

In private clouds, enterprises usually use their own (proprietary) data center to take the benifit of cloud computing while inside their firewalls.

[13]Alberto Fernández et al focus on the system for large-scale analytics based on the MapReduce scheme and Hadoop, its open-source implementation. It also identifies several libraries and software projects that have been developed for aiding practitioners to address this new programming model.This Cloud

Computing and its features stress its elasticity in the use of computing resources and space, less management effort, and flexible costs.

Advantage:-
The perspective of deploying a huge cluster of machines configured such that the load can be distributed among them.

Keqing He et al discuss about the Special Issue (SI) on Cloud Services Meet Big Data is to solicit innovative and promising methods and different techniques related to cloud services in the era of Big Data. The issue can promote the visibility and relevance of this noteworthy direction in the interdisciplinary field between Services Computing and other emerging disciplines.

Advantage:-
The evaluation of state-of-the art, using both real-world QoS data and synthetic Web service data.

[12]Marcos D. Asuncion et al discusses approaches and environments for carrying out analytics on Clouds for Big Data applications. Itencircles around four main areas of Big Data analytics, namely (i) data management and supporting architectures; (ii) model development and scoring; (iii) visualization and user interaction; and (iv) business models.

Advantage:-
Managing and gaining insights from the produced data is a key to competitive benefit.

III. Technologies Used:-

Pretty Good Privacy (PGP):-

Pretty Good Privacy (PGP) was originally developed by Phillip Zimmerman to provide a means of secure communication in an insecure electronic environment. The term "Pretty Good" is an underestimated framework which is based on, Public Key Infrastructure (PKI) and its encryption standards. It can use Diffie-Helman or RSA algorithms of varying strengths that have been subjected to rigorous cryptanalysis[16].

When a user encrypts plaintext using PGP, then PGP initially compresses the plaintext. Data compression saves modem transmission time, disk space, and more importantly, strengthens the security. Most cryptanalysis techniques accomplish patternsthat are present in the plaintext to crack the cipher. Compression reduces the patterns in the plaintext, thereby greatly enhancing resistance to cryptanalysis[15, 16].

PGP Encryption-

Then PGP creates a session key, which is a one-time-only secret key. This key is a random number generated by the random movements of your mouse and the keystrokes you type. This created session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; and generated result is cipher text.

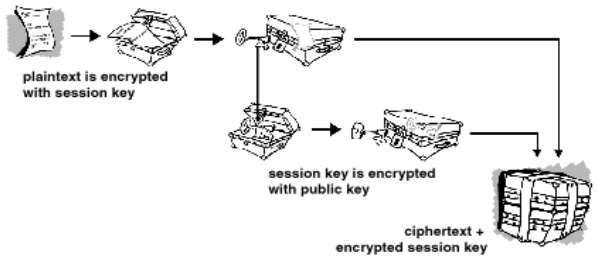

Figure: - PGP Encryption.

Earlier the data is encrypted the session key is again encrypted to the recipient's public key. This public key-encrypted session key is then transmitted along with the cipher text to the recipient[15].

PGP Decryption-

Decryption works in the reverse process. The recipient's copy of the PGP uses his or her private key to recover the temporary session key. Then the PGP decrypt the conventionally-encrypted cipher text.

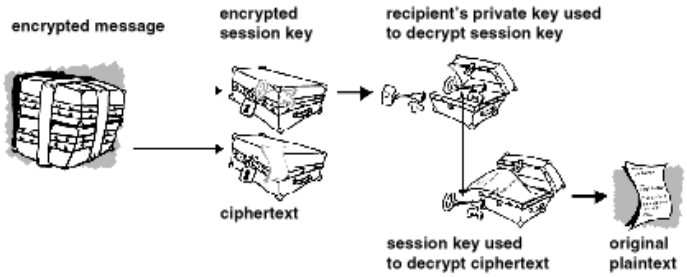

Figure: - PGP Decryption.

Real-trust Trust Degree (RTD)

RTD is used to evaluate recent cloud resource service operators, and RTD is evaluated by knowledge of a resource's quality of service. Hence, RTD is a time window-based trusted indicator for service operators, and it should be more sensitive to new operators. RTD is generated in the time period when an interaction takes place among a user and a resource respectively. This approach may lead to misinformation and could preclude an accurate evaluation of trustworthiness [2]. Thus, avoiding the effect of individual favoritism on the weight allocation of trust attributes is a key task. An adaptive trust evaluation model based on information entropy [5], which can overcome the shortage in traditional trust models, wherein the trusted attributes are weighted manually or subjectively.

IV. Advantages

1. Provides trustworthy & secure cloud service to the user.
2. Calculate real-time trust value of cloud resources at the different time.
3. Provide access control mechanism to the cloud services.

V. Conclusion

This paper is a survey of Intercloud Control and Management Plane that supports cloud based applications and infrastructure Services interaction; Intercloud Federation Framework that defines infrastructure components for independent cloud filed federation; and Intercloud Operation Framework that defines functional components and procedures to support cloud based services and operations. Research work of different researchers is explored in literature survey with its advantages. Different technologies that are used for big data analysis using parallel trust Computing is also demonstrated.

Acknowledgment

The authors would like to thank the publishers and researchers for making their resources available. We also thank the college authority for providing the required infrastructure and support.

References

[1]. David Bernstein and Deepak Vij "Intercloud Security Considerations"International Conference on Cloud Computing Technology and Science 2010 IEEE.
[2]. X. Li, F. Zhou, X. Yang, "A Multi-Dimensional Trust Evaluating Model for Large-scale P2P Computing", Journal of Parallel and Distributed Computing, vol.71, no.6, pp.837-847, 2011.
[3]. ShirleiAparecida de Chaves, Rafael BrundoUriarte, Carlos Becker Westphall "Toward an Architecture for Monitoring Private Clouds" 2011 IEEE.
[4]. H. Shen and G. Liu, "An efficient and trustworthy resource sharing platform for collaborative cloud computing," IEEE Trans. Parallel Distributed. System., vol. 25, no. 4, pp. 862–875, Apr. 2014
[5]. H. Zhou, G. Zhang, G. Wang, "Multi-objective decision making approach based on entropy weights for reservoir flood control operation", Journal of Hydraulic Engineering, Vol. 38, no. 1, pp. 100-106, 2007.
[6]. F. Paraiso, N. Haderer, P. Merle, R. Rouvoy, and L. Seinturier, "A federated multi-cloud PaaS infrastructure," in Proc. 5th IEEE Int. Conf. Cloud Comput. (CLOUD), Jun. 2012, pp. 392–399.
[7]. Hamid MohammadiFard, RaduProdan and Thomas Fahringer "A Truthful Dynamic Workflow Scheduling Mechanism for Commercial Multi-Cloud Environments" TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 2012 IEEE.
[8]. Xiaoyong Li, Huadong Ma, Feng Zhou and XiaolinGui "Service Operator-aware Trust Scheme for Resource Matchmaking across Multiple Clouds" 2013 IEEE.
[9]. I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, "Cloud-centric multi-level authentication as a service for secure public safety device networks," IEEE Commun. Mag., vol. 54, no. 4, pp. 47–53, Apr. 2016.
[10]. Y. Demchenko, M. X. Makkes, R. Strijkers, and C. de Laat, "Intercloud architecture for interoperability and integration," in Proc. IEEE 4th Int. Conf. Cloud Comput. Technol. Sci. (CloudCom), vol. 1. Dec. 2012, pp. 666–674.
[11]. D. Niyato, Z. Kun, and P. Wang, "Cooperative virtual machine management for multi-organization cloud computing environment," in Proc. Int. Workshop Game Theory Commun. Netw. (Gamecomm), Paris, France, May 2011, pp. 528–537.

[12]. M. Singhal et al., "Collaboration in multicloud computing environments: Framework and security issues," Computer, vol. 46, no. 2, pp. 76–84, 2013.
[13]. Alberto Fernández, Sara del Río,VictoriaLópez, Abdullah Bawakid, María J. del Jesus, José M. Benítez and Francisco Herrera "Big Data with Cloud Computing: an insight on the computing environment, MapReduce, and programming frameworks" © 2014 John Wiley & Sons, Ltd. Volume 4, September/October 2014.
[14]. Ali Gholami and Erwin Laure "BIG DATA SECURITY AND PRIVACY ISSUES IN THE CLOUD" International Journal of Network Security & Its Applications (IJNSA) Vol.8, No.1, January 2016.
[15]. https://www.slideshare.net/pavanaarrya/pgp-pretty-good-privacy.
[16]. https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html - imp PGP working.