ISSN 2347 - 3983

Volume 8. No. 7, July 2020

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter64872020.pdf

https://doi.org/10.30534/ijeter/2020/64872020

Extended OpenStack Architecture for Enforcing Comprehensive Security within Cloud Computing System

Dr. JKR Sastry, B. TrinathBasu

[1]KoneruLakshmaiah Education Foundation, Vaddeswaram, India, drsastry@kluniversity.in

[2]KoneruLakshmaiah Education Foundation, Vaddeswaram, India, miriiyala68@kluniversity.in

Many business enterprises are migrating to the cloud computing system due to inherent advantages and also a significant reduction in the cost of providing IT solutions. While that being the case, the Security of the user's data and applications isa significant concern as the user's IT assets are physically located and managed by third-party service providers. The architecture presented in the literature does not contain the components that are required to ensure full complicate to the security requirements of the users.

In this, an architectural model that satisfies the security requirements of users considering every aspect has been presented.The comparative model has been sued for establishing the existing architectures and come out with the kind modifications that must be made to OpenStack so that OpenStack will be more comprehensive and fully secured.

Key words: Cloud Computing. Federation, Tokenization, Data Isolation, user-defined policies, and access control

1. INTRODUCTION

Cloud computing is a service model deployed over the internet to provided services to the end-users. The main objective of cloud computing technology is to ensure availability, high reliability, and scalability of infrastructural facilities, which include hardware, software, platforms, services, and software that could be distributed to different computing locations.

No standard definition as such has been defined and being followed as yet. A cloud computing platform is expected to provide reliable services in a distributed environment. The infrastructure which is used for building the cloud needs to be scaled seamlessly.

Every cloud should satisfy five different characteristics, which include Ubiquitous network access, Pooling distributed resources, on-demand service, compute the extent of service provided, and the ability to scale up as necessary.

Every cloud must support there delivery models that include Infrastructure as a Service, Platform as a Service, and Software as a Service. The cloud computing platforms should be either deployed as Private cloud, public cloud, hybrid cloud, and community cloud.

Conceptually a cloud is entirely service-oriented. Anything required by the cloud is delivered as a service. Hardware, software, platform, application software, system software, and utilityprovided in terms of the service.

Many cloud computing facilities created providing different kinds of services. One of the gravest concerns is the lack of a standard API and usage model. Cloud computing, as such, emerged out of the technologies that have come up over time. That technologies that lead to cloud computing include Distributed Computing, Utility computing, Grid Computing, Cluster Computing, and Virtualization. Designing a proper architecture that shall be used for the development or the expansion of the cloud infrastructure, proving the services and resources as per the quality as stated in service level agreements, is the most crucial issue to be addressed. One of the features of a cloud is to ensure that the confidentiality of the user data, process, software, applications, etc. is not lost.

The cloud computing architecture must support various types of users (providers, enterprises, and regular users) and should reflect the issues of scalability, infrastructure, storage, Security, services, and platforms. The architecture must deal with requirements of all types of users and also confirming to the individual security requirements that may differ from user to user.

This paper presents a comparative analysis of the existing architectures. It brings out the extent to which security enforcement as per the users' requirement has been covered. Also, itoffers an architecture that shows the way user-defined security requirements have been considered about data storage and retrieval, resource allocation, that satisfies the service level agreements.

2. PROBLEM DEFINITION

The main problem thus is defined as an architecture using which a cloud computing system can be built such that user can specify the policies and access control that must be effected within the cloud computing system

The problem is also making the cloud computing systems e federated with the existing well-proven and secured authentication system.

The problem is also related to protecting the secrecy of the data when Multi-tenancy is used.

3. RELATED WORK

Various kinds of components considered into a cloud computing system architecture, which essentially explains the way the components are structured and the way the communication happens among the components. The components considered and placed in the architecture include cloud resources, services, middleware, application, and system software.

Nothing about the hardware, as such, is described in architecture. The architecture explains the properties of the software objects and the relationships between the objects. The architecture that defines the cloud computing infrastructure shall deal with various aspects that include Structures, platform adaption, structuring cloud services, and cloud components, the relationship between multiple components, Communicating between the objects, middleware that addresses the heterogeneity among the communicating objects or to work as a broker between the user and the backend computing system, Deploying and managing security components and to check various legal issue primarily when related to exporting data across the continents[1].

Many components exist within the cloud infrastructure. Data storage and retrieval are made available as a service to the user. When it comes to the data, confidentially of the same is essential.

Every component has an architecture built into overall cloud computing architecture. Many storage devices that are either supported on the servers or the network storage devices e clustered to form the total storage.

Dedicated software running on one of the servers is made responsible for managing the storage in terms of allocation, storing the user data, and retrieval of the data as per user requirements. The software also deals with providing access rights to the user for availing the data services and revoking the same when the service is completed.

Security has been the most critical issue when it comes to data storage and retrieval and also transmitting the same to the end-user over the internet. Safety is also the issue when the Data transfer from the user to the cloud implemented. Cloud storage is not just the data supported on a server as in a conventional system.

Cloud storage, as such, includes network devices, storage devices, servers, applications, public access interfaces, client programs, and similar such systems. A sub-system implemented that manages storage in the cloud computing environment.Clustered storage architecture is generally performed for providing efficient storage services and also to support scalability and fault-tolerant data storage and retrieval systems.

The cloud storage resources are organized as a cluster, a grid, or a distributed file system. The connecting network and the storage management software together provide the data storage services to the end-users. Providing the user the easy access and high-performance data services are the main objectives of cloud computing systems when it comes to data storage and retrieval. The storage infrastructure provided in cloud computing systems is homogenous and supported on homogenous platforms while that not being the case now. A heterogeneous cloud storage infrastructure management has been presented [2]

Customers enter into service level agreements (SLA) with cloud computing service providers for want of various kinds of services that are related infrastructure, platform, and software provisioning. The services differ a lot from user to user. Resource management systems generally do not follow SLA for managing the resources leading to some kind of rendering fewer quality services to the end-users. SLA based resource allocation provides a very high quality of data storage services.

Customer-driven approaches are mostly needed for providing quality services to the end-users. The customer-oriented service management, management of computational risk, autonomic resource management needs to be integrated into market-based resource management. This will help in adapting to the rapidly changing services requirement scenario. The architecture presented considers the control of the requirements perSLAs. The architecture proposed is based on market-driven policies and virtualization technologies, which supports providing a flexible allocation of services [3].

Virtualized services that are dynamically scalable provided to the users through a service model supported by cloud computing technologies. No standard, as such, exists as on date for implementing cloud computing solutions. Much architecture used for building cloud computing systems. The requirements of the users are to be found first and then classify the same based on some criteria. It has been shown that some features required by the users, such as the requirements for storage, software, platform, securing the data, etc., play a vital role in defining the architectures which should be used for building cloud computing infrastructure [4].

As said earlier, providing data storage and retrieval related services has been one of the essential services offered by many of the service providers. Google Drive, one drive, etc., are some of such services. A separate architecture has been on the anvil to support such a facility. Several storage technologies such as HDFS (Hadoop distributed file system), GFS (google file system), MapReduce, Big Table, etc. are to be considered for finalizing the architecture. A method that improves the conventional file storage system based on the eye-OS WEB operating system presented that not only implements distributed storage and also achieves the control to make the system fault-tolerant [5].

Many clouds are in use these days, and each cloud provides some services. The user requirements can only be serviced sometimes through the services offered by a set of cloud computing systems. Inter-cloud operations are required in that case. The architecture involving multiple clouds must address numerous providers, numerous domains, heterogeneous applications, and the need for application integration, supporting legacy services and interoperability.

A cloud computing system makes the users independent of physical hardware, platform, distributed computing platforms, and networking technologies. NIST Cloud Computing Reference Architecture (CCRA) is one of such architectures offered for implementing inter-cloud services. Based on NIST, an inter-cloud design has been proposed that focuses on interoperability and integration.

The architecture is built using multiple service models,which include SaaS, Paas, and IaaS.

A separate layer is designed for locating a service model. Communication between the layers carried using suitable interfaces. A separate system takes care of Inter-cloud Control and management of communication between the applications running on different clouds

An architectural framework is presented that provides the basis for building multilayer cloud services, optimized provisioning of computing, storage, and networking resources. Architecture is presented that facilitates cloud interoperability and integration [6].

A cloud constructed involving multiple providers using the resources isspread across various domains, including the legacy infrastructures and services. Resources are made available to the users on demand through Virtualization of the resources. Some times, multiple clouds are needed when one wants to convert existing infrastructure into cloud-based infrastructure. An architecture that deals with various clouds with the interface between the clouds needs to be developed.

The multiple clouds developed must be interoperable. New service provisioning models, security models are required to provide services to end-user on demand. Virtualization is one mechanism that helps in moving the existing infrastructure or add-ons into cloud-based infrastructure.
There are significant benefits that one will accrue when the migration of the existing infrastructures or WEB-based services to cloud-based infrastructure and services is undertaken, especially considering elastic scaling and on-demand provisioning.

Several functionalities added in terms of the addition of services that can operate on multiple clouds. These additional functionalities are to be inserted into inter-cloud architecture. Inter-cloud architecture should address various issues that include the following:

1. Provide the services considering every cloud independently and also have a mechanism that measures the usage of the resources by end-users
2. Integration and interoperability of multiple clouds including the integration of legacyinfrastructure
3. Provide the services considering Multiple clouds (cloudFederation)

An architectural framework has been presented for operating a system that uses multiple clouds. Many users world over are moving from traditional client server-based computing to cloud-based computing due to the essential services offered. On-demand service provision is one such criterion. The use of cloud computing infrastructure is evident while at the same time, many and different clouds expected to be created and operated. It becomes necessary to provide services to the end-users considering multiple clouds at the same time as a matter of federation.

AT times the same service can be availed from multiple vendors. Reference architecture (RA) required when services provided through either of the clouds are established using inter-cloud interaction. A multi-cloud reference architecture (RA) is presented that allows a user to use services provided by any of the vendors, such as data storage services offered by either Google or Microsoft. A comparison of the RA presented is made against the RA of the National Institute of Standard Technology (NIST)[7].Cloud computing is all about sharing the resources such as processors, servers, storage, memory, bandwidth, services, applications that can be provided as services on demand and release the same on completing the service.

The allocation and de-allocation are done with minimal management requirements. After the era of WEB based processing, cloud computing has come in a big way. Cloud computing has come into force due to the amalgamation of many old technologies such as SOA, Grid Computing, distributed computing, and Virtualization. Resources that are connected to several servers that are geographically spread across represented as a pool of computing resources that are made available on demand.

The resources typically comprise memory, storage, processors, bandwidth, etc. The resources in the pool can be either be made to shrink or expand in real-time so that the desired levels performance, scalability, reliability, latency, sensitivity, Security ensured. The resources are made available to the user on-demand as a logical unit called "Cloud Computer."

The cloud model as such can be composed using four deployment models (public, private, Hybrid, community), three service models (Iaas, PaaS, SaaS), and five essential characteristics (on-demand self- service, broad network access, resource pooling, rapid elasticity, measured service).

A cloud provider usually enters into service level agreements that include not only pricing but also the quality of service provided to the end-users. SLA also consists of the penalties that the service provider takes if the service provider fails to ensure the quality of the service that they have committed. The service provider is equally concerned with running the cloud computing facility by consuming minimum energy and excellent resource utilization through constant monitoring and taking corrective actions wherever required.

The concept of software-defined clouds has been presented that helps to configure the cloud optimally by extending the idea of Virtualization to all the pooled resources. The concept of Virtualization, as such, is extended to only physical machines earlier.

The demands of QoS are met through software-defined clouds. SDC can manage various aspects of cloud computing such that QoS requirements could be achieved. The architecture used for implementingSDC that caters to mobile cloud-based applications.

The architecture has been evaluated from two perspectives that include bandwidth allocation, energy-efficient VM placement [8]. The architecture is developed over software-defined networks (SDNs, Server and Network Virtualization, software-defined, and middlebox networking. It has been shown the way these different technologies are combined to form SDC.

4.REVIEW OF EXISTING ARCHITECTURES

Gerald Kaeferet al. [1] recommended two architecture,which shown in figure 1 and Figure 2.It can be seen from Figure-1 and Figure 2 that the issue of Security is enforced at the Services layer only.

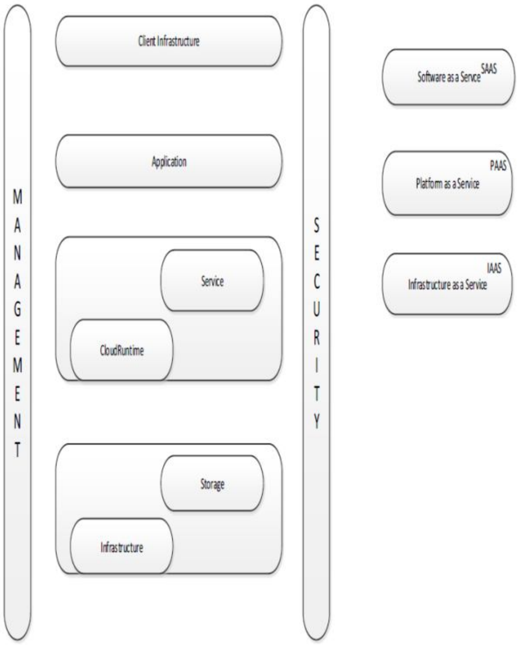

Figure 1:Grald Kaefer Architecture -1

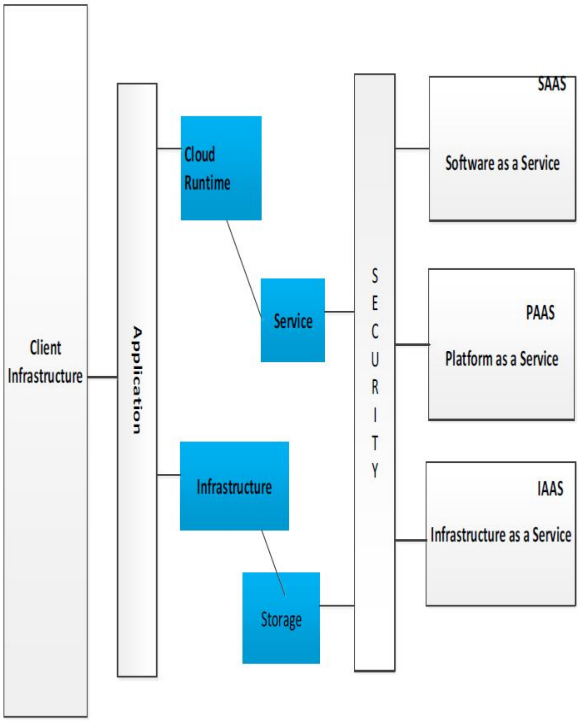

Figure 2: Grald Kaefer Cloud computing Architecture-2

The architecture proposed by Dejun Wang et al., [2] is shown in figure 3. Security provision in this architecture is limited to user names and passwords only.

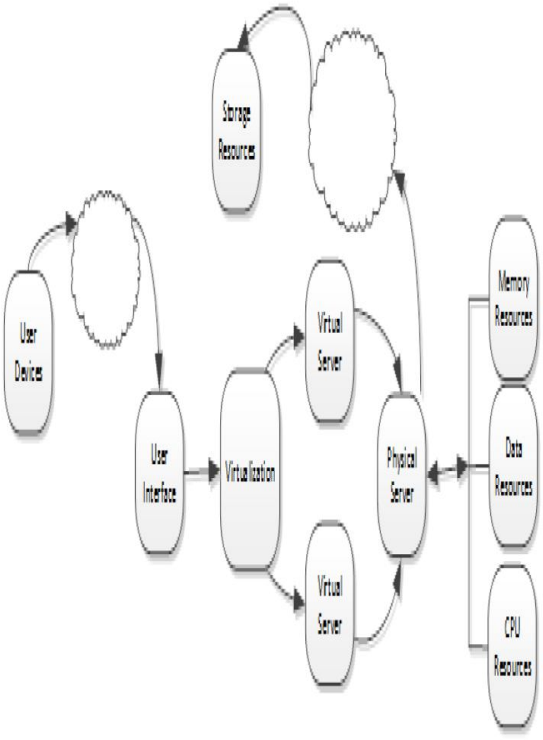

Figure 3: Dejun – Cloud Computing Architecture

The architecture proposed by Raj Kumar Buyya et al., [3] is shown in figure 4. From the architecture, it can be seen that security infrastructure support is made available through a separately provisioned component that can be used by the users to protect their data in addition to the User Name Password-based access provided to the users.

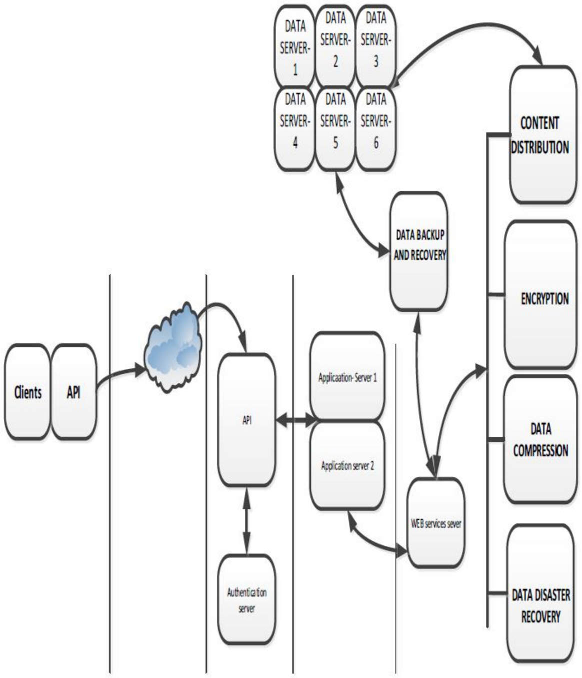

Figure 4: Raj Kumar Buyya – Cloud computing architecture

Bhaskar Prasad Rimal et al. [4] have proposed architecture shown in Figure 5. From the figure, it can be seen that Security is provided to secure information submitted to various services in addition to the provision made through user names and passwords.

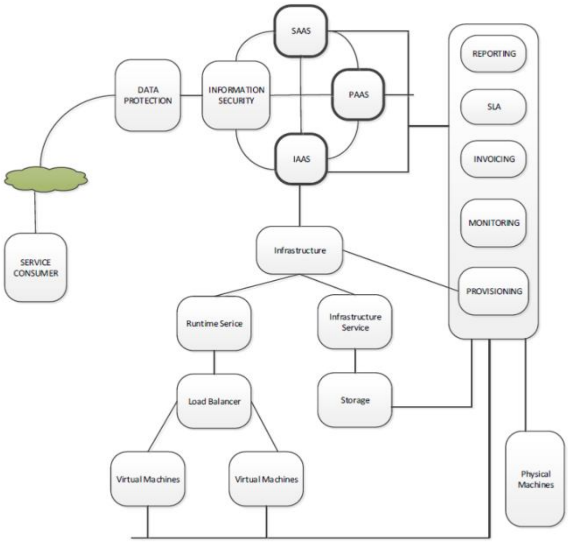

Figure 5: Cloud computing architecture - Bhaskar Prasad

The architecture proposed by Kun Liu et al. [5] isshown in Figure 6. The architecture just explains the way the data is handled between the user and the cloud. No security feature as such incorporated into the architecture security provision, in this case, is limited to the User name and password protection

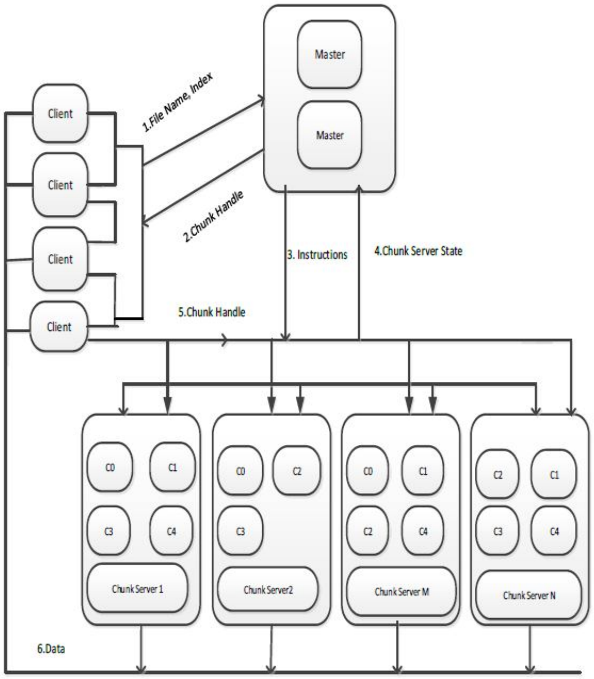

Figure 6: Kin Liua –Architecture

Yuri Demchenko et al., [6] have proposed an architecture shown in Figure 7. No security provision, as such, has been incorporated into the architecture except for traditional user name and password-based protection.

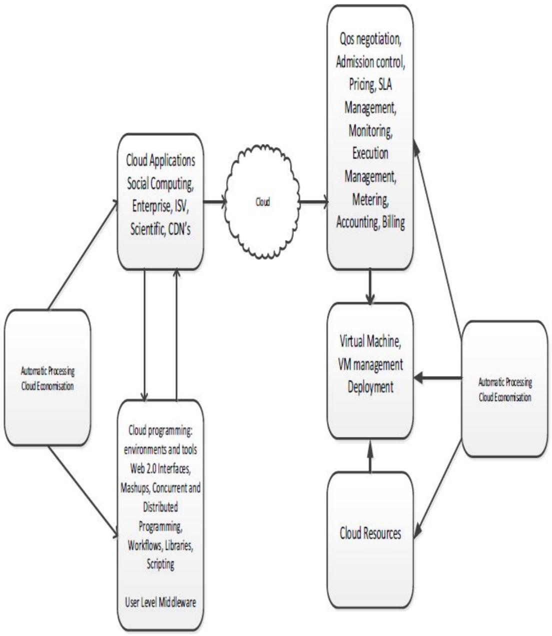
Qos negotiation, Admission control, Pricing, SLA Management, Monitoring, Execution Management, Metering, Accounting, Billing
Cloud Applications Social Computing, Enterprise, ISV, Scientific, CDN's
Cloud
Automatic Processing Cloud Economisation
Virtual Machine, VM management Deployment
Automatic Processing Cloud Economisation
Cloud programming: environments and tools Web 2.0 Interfaces, Mashups, Concurrent and Distributed Programming, Workflows, Libraries, Scripting
User Level Middleware
Cloud Resources

Figure 7: Yuri Demchenko Architecture

The architecture proposed by Raj Kumar Buyya et al., [7] is shown in Figure 8. No security provision, as such, made into the architecture.

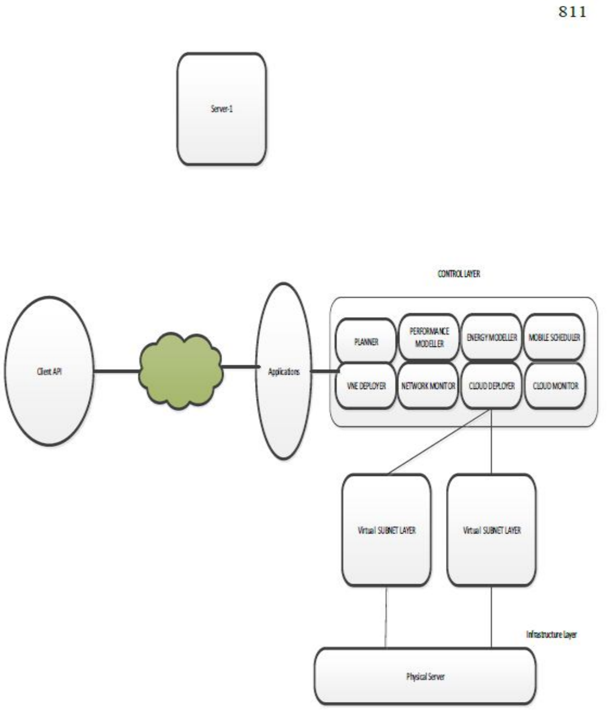

Figure 8: Raj Kumar Buyya – Architecture 2

The architecture presented by DemekeGebresenbetBayyou et al. [8] shown in figure 9. No security provision made in this architecture except for username + password-based protection

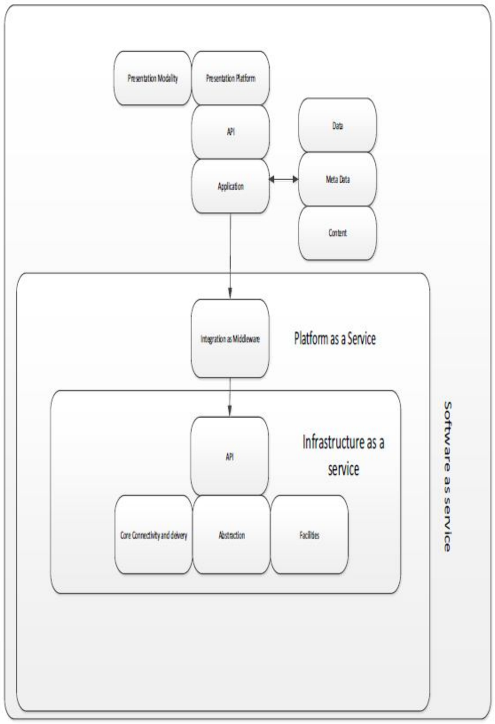

Figure 9: Cloud computing architecture - Demeke Gebresenbet Bayyou

The Architecture implemented in OpenStackshown in Figure 10. From the figure,it is seen that Security to the extent of authentication, authorization, access control, and fine-grained policy-based Data security provisions have been incorporated. However,many vulnerabilities exist in the arrangements made into the architecture of OpenStack.

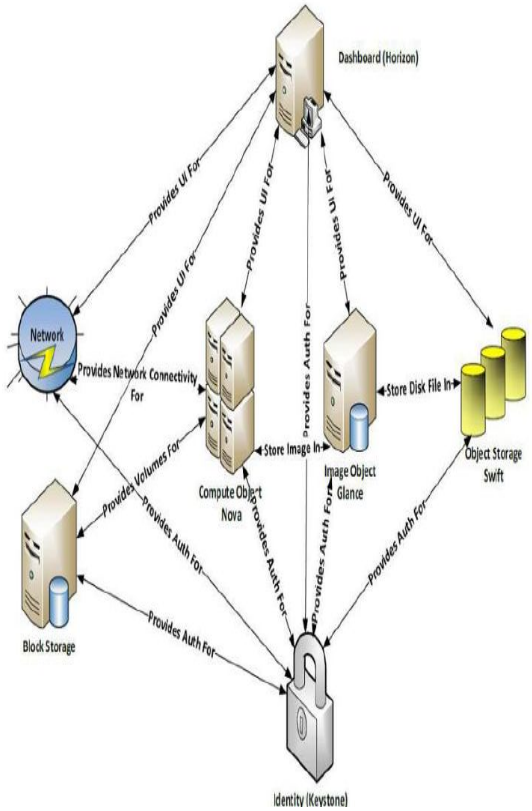

Figure 10 OpenStackArchitecture

5.COMPARATIVE ANALYSIS

The architectures presented above have been analyzed to find the extent to which the architectures fulfilled the requirements of a full security enforcement system. The following security enforcement parameters have been considered for affecting the comparisons. Table-1 shows the comparison.

1. User name + Security provision
2. Service-level security enforcement
3. Identify based security enforcement
4. Implementation of user-defined and system-defined access control
5. Exercising access control based on user-defined and system-defined polices.
6. Data security enforcement considering different types of storage systems that include conventional databases, Object stories, and volume-based storage
7. Implementation of federation with existing well-proven Authentication systems like IMS and ADDS
8. Implementation of advanced tokenization system like JSON

9. Data isolation at different levels
10. Support of Security infrastructures suchas the generation of keys and certificates and validation of certificates.

From the Table,one can see that none of the existing architectures are fully comprehensive that every aspect of security enforcement could be covered. OpenStackincludes the majority of the requirements. Still, many of the advanced elements have not been supported, such as federation with existing, proven authentications system, dealing with user-defined policies, and access control. Inclusion of the latest tokenization system, data security under the issue of multi-tenancy, etc. needs to be included in the OpenStack architecture so that OpenStack-based cloud computing offered under a fully secured environment.

6.EXTENDED ARCHITECTURE

OpenStack architecture has been extended to add features related to user-defined access control and polices. Data isolation when multi-tenancyused, a federation of existing ADDS and IMS systems with keystone module of the OpenStack, implementation of JSON tokens in conjunction with fernet tokens implemented within OpenStack, Figure 11 shows the OpenStack extended architecture that Security of the user resources is made more comprehensive and extensive.

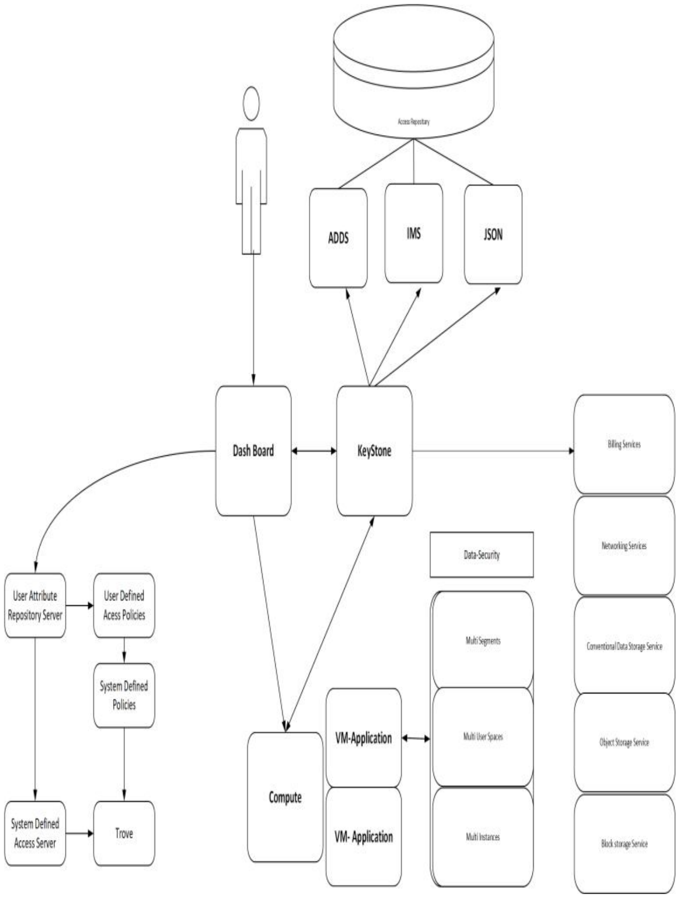

Figure 11: Extended OpenStack Architecture

7.CONCLUSIONS

One major drawback of most of the cloud computing systems is the inability to secure user data and applications fully. Users, as such, cannot dictate or decide the way their resources are to be secured. Users cannot as such the polices and access control mechanisms to be followed by the cloud computing systems

Federation with existing full proven authentication systems such as ADDS and IMS is the key to ensure comprehensive Security within cloud computing systemsThe use of sophisticated token systems that ensure full Security and, at the same make authentication system simple is the most critical aspect of a cloud computing system.

The aspect of data Isolation is critical,mainly when multi-tenancy is used. Data isolation achieved considering all types of storage systems that include conventional databases, object storage, and volume-based storage systems.

The architecture presented in this paper is comprehensive as all security requirements met through inclusion or components that seamlessly integrated with OpenStack components

REFERENCES

1. Gerald Kaefer, Cloud Computing Architecture, Corporate Research and Technologies, Munich Germany, 4th Generation Data canter IEEESpectrum,1-9,2010.
2. Dejun Wang, An Efficient Cloud Storage Model for Heterogeneous Cloud Infrastructures, JOURNAL,1877- 7058/10.1016, 510-515,2011.
3. RajkumarBuyya, Saurabh Kumar Garg, and Rodrigo N. Calheiros, SLA-Oriented Resource Provisioning for Cloud Computing: Challenges, Architecture, and Solutions,2011 International Conference on Cloud and Service Computing,1- 10,2011.
4. BhaskarPrasadRima, AdmelaJukanDimitrios,and KatsarosYvesGoeleven,ArchitecturalRequirementsforCloudComputing,JOURNAL/10.1007/DOI10.1007/s10723-010-9171-y,1-26,2011.
5. KunLiu,Long-JiangDonga,"ResearchonCloudDataStorageTechnologyandItsArchitectureImplementation," JOURNAL/1877-7058/10.1016,133-137,2012.
6. Yuri Demchenko, Canh Ngo, Marc X. Makes, Rudolf Strijkers, 1Cees de Laat, Defining Inter-Cloud Architecture for Interoperability and Integration, CLOUD COMPUTING 2012: The Third International Conference on Cloud Computing, GRIDs, and Virtualization, ISBN:978-1-61208-216-5,1-7,2012
7. DemekeGebresenbetBayyou, Menchita F, Dumlao, Cloud Computing Reference Architecture from

Different Vendors Perspectives, International Journal of Emerging Technology and AdvancedEngineering,Volume 3, Issue11, page 1-7,2013.

8. RajkumarBuyya, Rodrigo NCalheiros, Jungmin Son, Amir VahidDastjerdi, Young Yoony,SoftwareDefined Cloud Computing-Architectural Elements, and Open Challenges,3rd International Conference - Advances in Computing Communications and Informatics (ICACCI), Page 1-12,2014.
9. M. TrinathBasu, Dr.JKRSastry, A full security included Cloud Computing Architecture, International Journal of Engineering & Technology, Volume 7, Issue 2.7, Page 807-812, 2018
10. M. TrinathBasu, JKRSastry, Improving the OpenStack Authentication system through federation with JASON Tokens, International Journal of Advanced Trends in Computer Science and Engineering, Volume 8, Issue 6, Pages 3596-3614,2019 https://doi.org/10.30534/ijatcse/2019/143862019
11. TrinathBasu, JKRSastry, Strengthening Authentication within OpenStack Cloud Computing System through Federation with ADDS System, International Journal of Emerging Trends in Engineering Research, Volume 8, No. 1, Page, 213-238, 2020 https://doi.org/10.30534/ijeter/2020/29812020
12. JKRSastry, M TrinathBasu, Multi-Factor Authentication through Integration with IMS System, International Journal of Emerging Trends in Engineering Research, Volume 8, No. 1, Page, 88-113, 2020 https://doi.org/10.30534/ijeter/2020/14812020
13. J. K. R. Sastry, K. Sai Abhigna, R. Samuel and D. B. K. Kamesh, Architectural models for fault tolerance within clouds at the infrastructure level, ARPN Journal of Engineering and Applied Sciences, VOL. 12, NO. 11, 2017, Pages 3463-3469
14. DBK Kamesh, JKRSastry, Ch. Devi Anusha, P. Padmini, G. Siva Anjaneyulu, Building Fault Tolerance within Clouds at Network Level, International Journal of Electrical and Computer Engineering (IJECE), Vol. 6, No. 4, pp. 1560~1569, 2016 https://doi.org/10.11591/ijece.v6i4.10676
15. S. L. SUSHMITHA, Dr. D. B. K. JKRSASTRY, V. V. N. SRI RAVALI, Y.SAI KRISHNA REDDY, building fault tolerance within clouds for providing uninterrupted software as service, Journal of Theoretical and Applied Information Technology, Vol.88. No.1, Pages 65-76, 2016
16. JKRSastry, M TrinathBasu, Securing Multi-tenancy systems through user spaces defined within the database level, Jour of Adv Research in Dynamical & Control Systems, Volume 10, issue 7, Page 405-412, 2018
17. JKRSastry, M TrinathBasu, Securing Multi-tenancy systems through multi DB instances and multiple databases on different physical servers, International Journal of Electrical and Computer Engineering (IJECE), Volume 9, Issue 2, Pages 1385-1392, 2019. https://doi.org/10.11591/ijece.v9i2.pp1385-1392
18. JKRSastry, M TrinathBasu, Securing SAAS service under cloud computing-based multi-tenancy systems, Indonesian Journal of Electrical Engineering and Computer Science, Volume 13, Issue 1, Page 65-71, 2019 https://doi.org/10.11591/ijeecs.v13.i1.pp65-71
19. M TrinathBasu, JKRSastry, Enhancing Data Security under Multi-Tenancy within OpenStack, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, Issue 1, 2020, pp .533-544 https://doi.org/10.30534/ijatcse/2020/73912020
20. Dr.JKRSastry, M. TrinathBasu, Enhancement of Security within OpenStack – Some measures, International Journal of Emerging Trends and Engineering Research, Volume 8, Issue 3, 2020, pp. 919-938. https://doi.org/10.30534/ijeter/2020/49832020

Table 1: Comparison of existing Architectures with reference to Security provisions required within Cloud Computing Systems

Architecture	User Name + password	Identity-based	Service Level Access Control	Access		Policy-Based Security		Token-Based Security		Data Isolation			Support Security Infrastructure	Integration with Latest Tokenization Systems	Integration with Existing Authentication Systems	
				System Defined Access Control	User-defined Access control	Service-based Security through Internal Policies	Service-based Security through User-defined Policies	Tokenized Control	Advanced Tokenized Control	Data Isolation at the conventional database	Data Isolation at Object Storage	Data Isolation at Block Storage			Integrated with ADDS	Integrated with IMS
Grald Kaefer Cloud computing Architecture – Architecture-1	√		√													
GraldKaefer Cloud computing Architecture – Architecture-2	√		√													
Dejun – Cloud Computing Architecture	√															
Raj Kumar Buyya – Architecture-1	√												√			
Cloud computing architecture - Bhaskar Prasad	√															
Kin Liua – Cloud computing architecture	√															
Cloud computing architecture - Yuri Demchenko	√															
Cloud Computing Architecture - Raj Kumar Buyya - Architecture-2	√															
Cloud computing architecture - Demeke Gebresenbet Bayyou	√															
OpenStack Architecture	√	√	√	√	**X**	√	**X**	√	**X**	**X**	**X**	**X**	**X**	√	**X**	**X**