International Journal of Multidisciplinary Approach and Studies

ISSN NO:: 2348 – 537X

Cloud Computing Challenges and Opportunities

Dr. Mohamed Abdelghader Morsi*, Eman Naji Mahmoud Fadoul, Esraa Mohammed Eshag Ibrahim***, & Mehad Mohammed Ibrahim Mohammed******

**Associate Professor, Alneelain University, College of Engineering and Head of Future Trends Department in Telecommunications and Post Regulatory Authority (TPRA). Khartoum, Sudan.*
***UG, Alneelain University, College of Engineering, Computer Section, Khartoum, Sudan.*
****UG, Alneelain University, College of Engineering, Computer Section, Khartoum, Sudan.*
*****UG, Alneelain University, College of Engineering, Computer Section, Khartoum, Sudan.*

1. ABSTRACT

This paper introduces the technology of cloud computing, and the challenges and opportunities associated with it, it also finds solutions for security and high cost issues.

In this paper we use the open source which is a tool to build an environment for cloud computing, it also solves the aforementioned cloud problems in addition to providing an enormous storage capacity.

2. INTRODUCTION

Cloud computing is a set of IT services that are provided to a customer over a network on a leased basis and with the ability to scale up or down their service requirements. Usually cloud computing services are delivered by a third party provider who owns the infrastructure. Cloud computing offers an innovative business model for organizations to adopt IT services without upfront investment [4].

Enterprises are driving towards less cost, more availability, agility, managed risk - all of which is accelerated towards Cloud Computing. Cloud is not a particular product, but a way of delivering IT services that are consumable on demand, elastic to scale up and down as needed, and follow a pay-for-usage model [15].

Despite the potential gains achieved from the cloud computing, the organizations are slow in accepting it due to security issues and challenges associated with it. Security is one of the major issues which hamper the growth of cloud [4].

3. CLOUD COMPUTING CHALLENGES

Following are the possible threats and challenges while choosing cloud computing technology:

3.1 Data Leakage

Basically, when moving to a cloud, there are two changes for customers' data. First, the data will be stored away from the customer's locale machine. Second, the data is moved from a single-tenant to a multi-tenant environment. These changes may raise an important concern

called, data leakage. This has become one of the greatest organizational risks from the security standpoint.

Some companies have thought of data leakage prevention DLP products. These products aim to ensure data confidentiality and detect unauthorized access to data [1].

3.2 Privacy

Cloud services are using the Internet as their communication infrastructure, as a result, cloud computing involves several kinds of security risks. Cloud providers often allow anyone to begin using cloud services. The relative anonymity of these usage models encourages spammers, malicious users and other hackers, who have been able to conduct their activities with relative impunity.

Generally, data encryption is a solution to ensure the privacy of the data in the databases against malicious attacks. But this is not enough when clients also prefer privacy protection from accessing to their data by the provider. The simple way to solve this problem is to find a cloud provider which users can trust; otherwise, using a private cloud is a very wise solution [1].

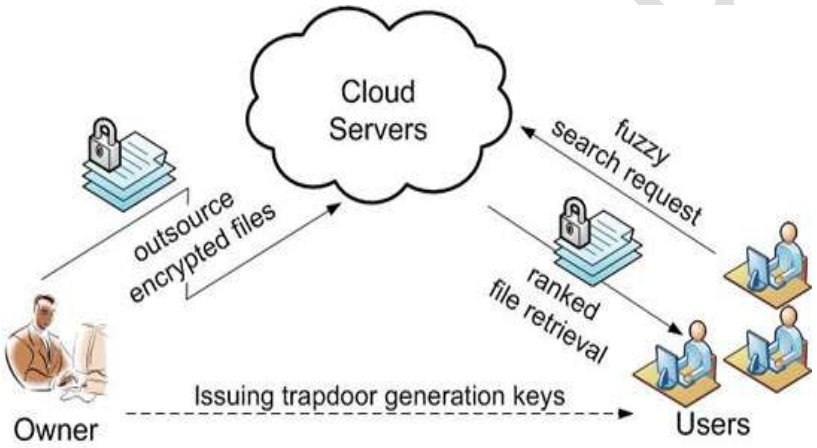

Figure (1): Privacy issue of cloud computing

3.3 Security

In cloud there are several security and privacy issues but in there are the Gartner's seven well-known security issues which cloud clients should advert are listed below [1].

- **Privileged user access:** information transmitted from the client through the Internet poses a certain degree of risk, because of issues of data ownership; enterprises should spend time getting to know their providers and their regulations as much as possible before assigning some trivial applications [5].
- **Regulatory compliance:** Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications.
- **Data location:** When clients use the cloud, they probably will not know exactly where their data is hosted. Distributed data storage is usually used by cloud providers,

but this can cause lack of control and is not good for customers who have their data in a local machine before moving to the cloud.

- **Data segregation:** Data in the cloud typically exists in a shared environment alongside data from other customers. Encryption is effective but is not a cure-all. While it is difficult to assure data segregation, customers must review the selected cloud's architecture to ensure data segregation is properly designed and available but without data leakage [1].
- **Recovery:** If a failure occurs with the cloud, it is critical to completely restore client data. As clients prefer not to let a third-party control their data, this will cause an impasse in security policy in these challenging situations [1]. So, every provider should have a disaster recovery protocol to protect user data [5].
- **Investigative support:** Cloud services are especially difficult to investigate because logging and data for multiple customers may be co-located and spread across an ever-changing set of hosts and data centres.
- **Long-term viability:** Ideally, a cloud computing provider will never go bankrupt or be bought by a larger company with new policies. However, clients must be sure that their data will remain available even after such an event [1].
- **Costing Model:** While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication, i.e. the cost of transferring an organization's data to and from the public and community Cloud and the cost per unit of computing resource used is likely to be higher.

The figure below show the security within cloud computing.

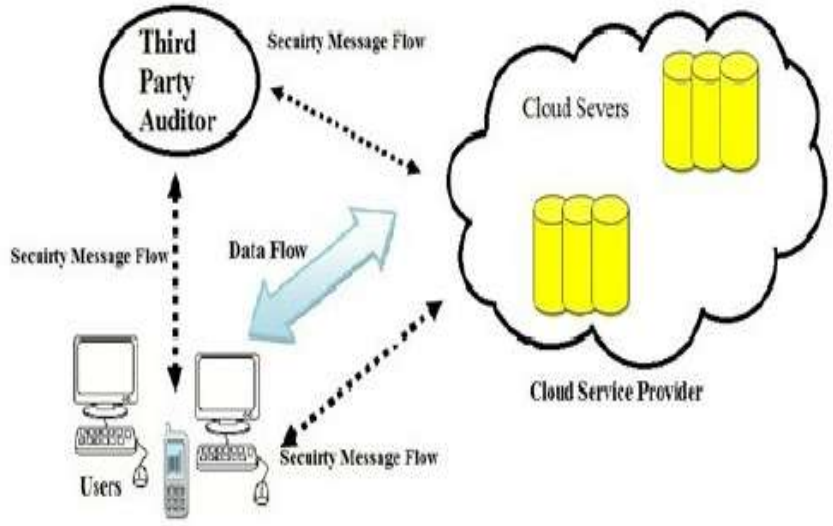

Figure (2): Security in cloud computing

3.4 Security solution in the cloud

There are traditional countermeasures against popular Internet security problems that may be usable in clouds, but some of them must be improved or changed to use in cloud environments[1].

1. Access Control

To ensure the accessibility of authorized users the prevention of unauthorized access to information systems, formal procedures should be in place to control the allocation of access rights to services.

Access control management to the host, network, and management applications that are owned and managed by the Cloud provider and user must manage access control to his virtual server, virtual storage, virtual networks, and applications hosted on virtual servers [1].

2. Private cloud

A private cloud offers the most control over security parameters because all security efforts are done in-house or are outsourced to managed security provider. [26]

3. Data encryption

To avoid access of data from other users, applying encryption on data that makes data totally unusable and normal encryption can complicate availability. Encryption is suggested as a better solution to secure information before storing it in cloud server. Data Owner can give permission to particular group member such that data can be easily accessed by them. Before uploading data into the cloud the users are suggested to verify whether the data is stored on backup drives and the keywords in files remain unchanged. [25]

4. FIND KEY CLOUD PROVIDER

First solution is of finding the right cloud provider. Different vendors have different cloud IT security and data management. A cloud vendor should be well established, have experience, standards and regulation. So there is not any chance of cloud vendor closing. [24]

4. Cloud computing opportunities

Following are the opportunities that the cloud offers to its clients:

4.1 User interaction

Interaction with users is scalable dependent on need and a cost model could be used based on how data is used.

4.2 Data sharing

With all information from the control system stored in a cloud, it allows for sharing the information with other unities. Clod computing also allows resource sharing.

4.3 Software updates

Cloud-based applications automatically refresh and update themselves, instead of forcing an IT department to perform a manual organization-wide update. This saves valuable IT staff time and money spent on outside IT consultation. PCWorld lists that 50 percent of cloud adopters cited requiring fewer internal IT resources as a cloud benefit.[27]

4.5 Life cycle

The hardware independence of the installed virtual machines gives a possibility to handle end of life of hardware components in a simpler way as long as they can be supported by the virtual machines.

4.5 Preprocessed platform

The cost of adding new person is not affected by the setup of the application, arrangement and installation for the new device, so there is no need to make changes on the platform for the new person or application to be added into it[11].

5. METHODOLOGY AND RESULTS

5.1 Environment

5.2 OpenStack services are installed onto two nodes (VMs), controller and compute.

Controller node runs the Identity service, Image service, management portions of Compute, management portion of Networking, various Networking agents, and the Dashboard. It also includes supporting services such as an SQL data base, message queue, and NTP.

Compute node runs the hypervisor portion of Compute that operates instances. The compute node also runs a Networking service agent that connects instances to virtual networks.

We used two processors, 4GB memory, and 100GB storage for the controller node, and two processors, 2GB memory and 100GB storage for compute node.

After installing the operating system on each node, we configured the network interfaces, NAT (management), and Host only (provider).

Management

Network requires a gateway to provide Internet access to all nodes for administrative purposes such as package installation, security updates, DNS, and NTP.

Provider network requires a gateway to provide Internet access to instances in the Open Stack environment. We assumed Management network interface to be 192.168.43.0/24, and the Default gateway is 192.168.43.1.

5.3 Installation and configuration of OpenStack services

The OpenStack system consists of several key services that are separately installed. These services work together depending on cloud needs and include the Compute, Identity, Networking, Image, Block Storage, Object Storage, Telemetry, Orchestration, and Database services. These services are installed and configured them separately.

5.4 Results

Result in figure (4) shows network topology consists of two networks; provider network and self service network, router connects the two networks, two instances; provider instance connected to provider network, and self service instance connected to self service network.

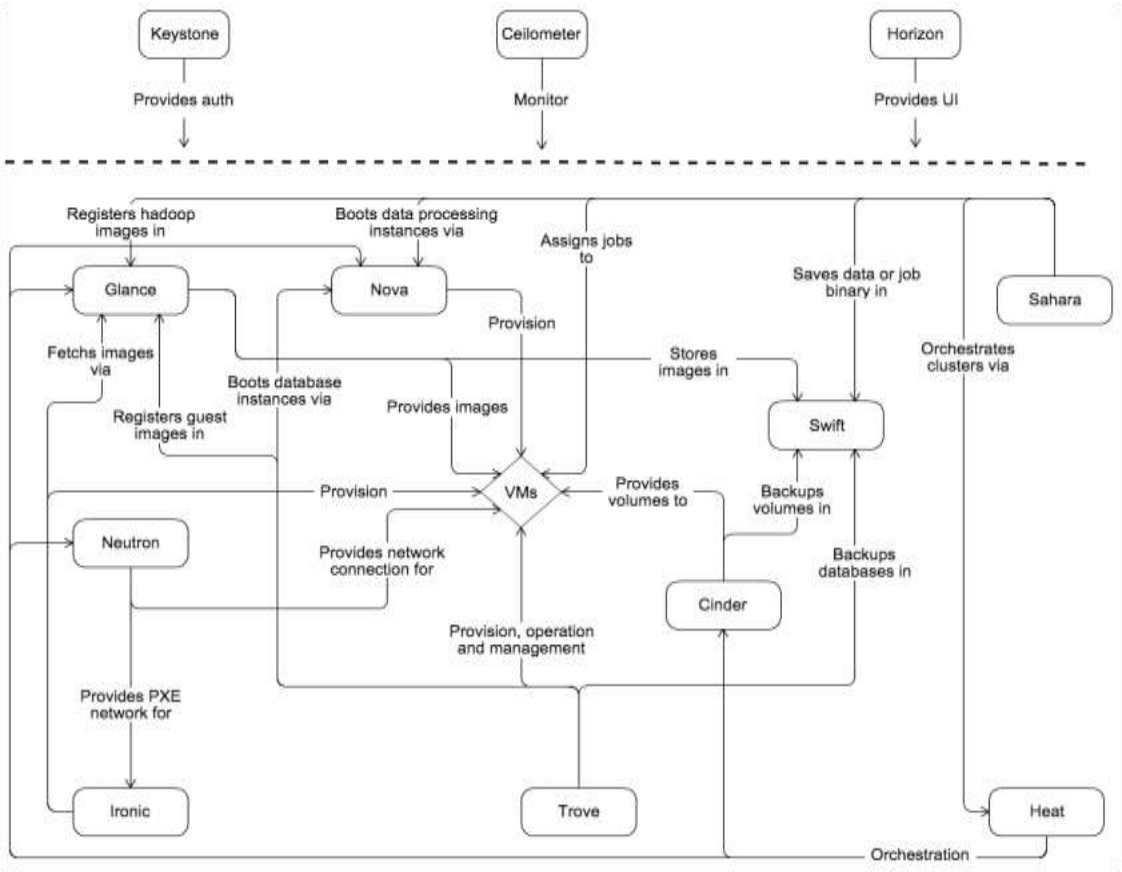

Figure (3): The relationships among the OpenStack services

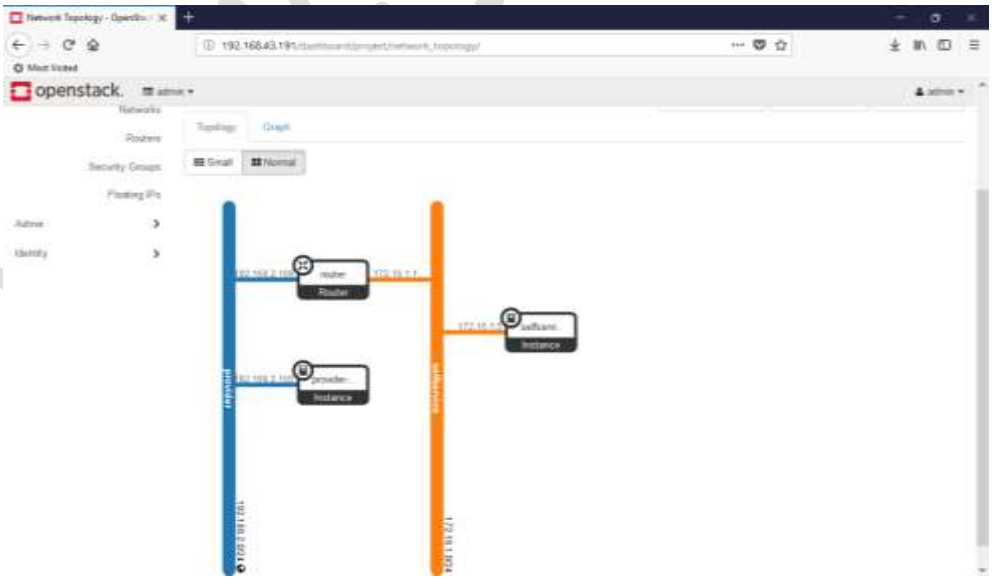

Figure (4): Network topology

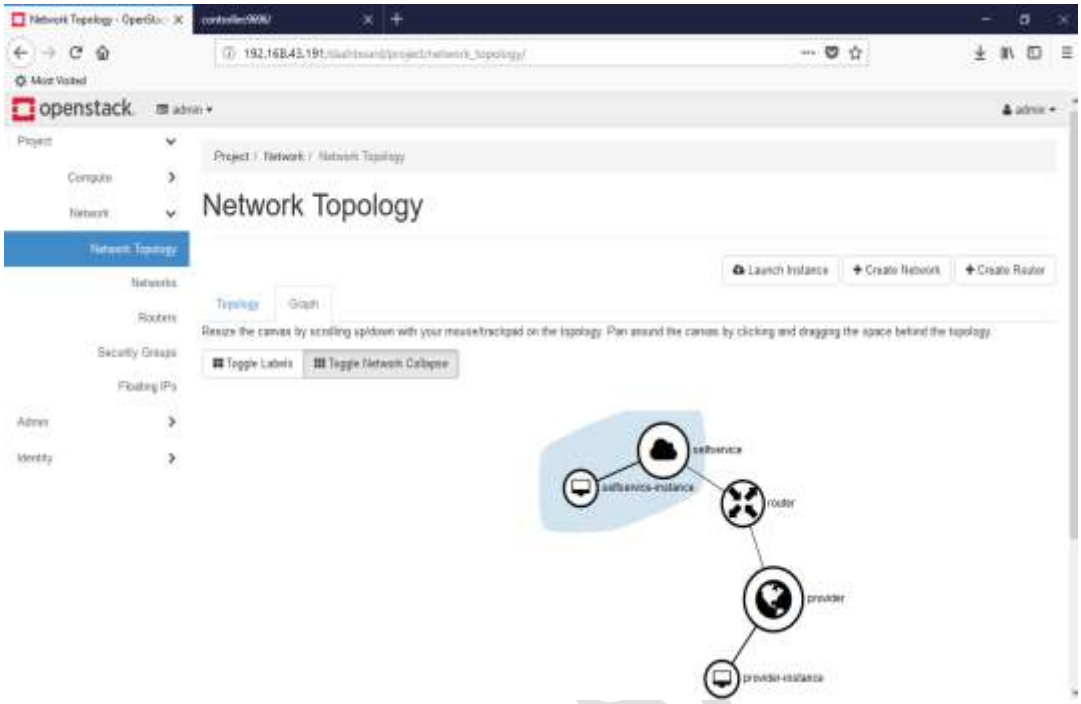

Figure (5) shows the network graph

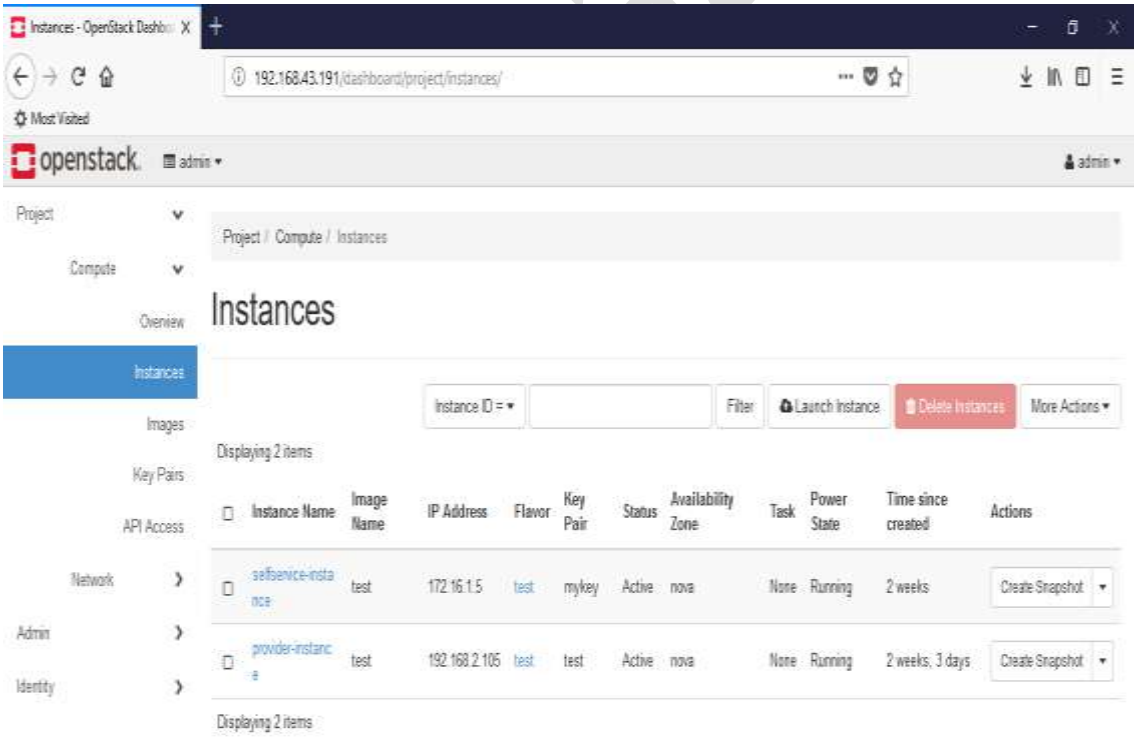

Figure (6): active status instances

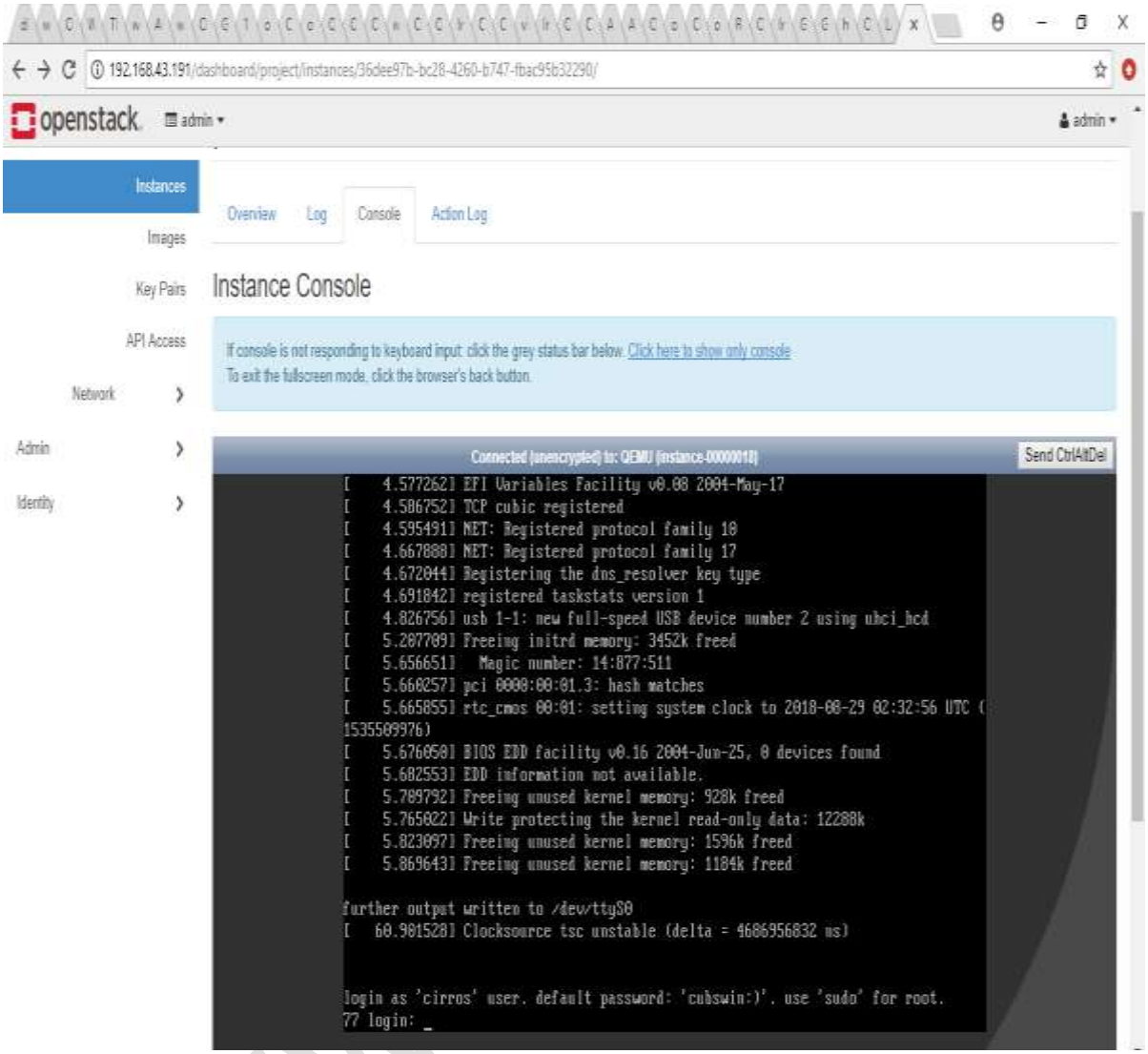

Figure (7): instance console

6. CONCLUSION

Cloud computing is one of the new technologies that needs to keep pace with development , it has a wide-ranging benefits as a form of computing that improves business execution through high scalability availability, reliability and also reducing overall costs to some extent. But relying on them is not without obstacle. Many users raise issues such as privacy and security when it comes to "cloud." There is therefore a growing interest in open-source cloud computing tools, which enable companies to build and customize their environments, greatly reduce costs, and apply more security techniques.

7. RECOMMENDATIONS AND FUTURE WORK

When installing Openstack services, consider repair hardware resources to your environment for the best performance.

We recommended developing the instances in openstack, getting the best out of its services.

As a developer, safety must be given great importance as an important issue in cloud environment.

Activate cloud computing services to serve educational process.
Consider encrypting the data for more privacy.

8. References

i. FarzadSabahi, " Cloud Computing Reliability, Availability and Serviceability (RAS): Issues and Challenges ".

ii. SandeepKelkar, "Challenges and Opportunities with Cloud Computing".

iii. Tharam Dillon & Chen Wu and Elizabeth Chang " Cloud Computing: Issues and Challenges.

iv. Kuyoro S. O., Ibikunle F. &Awodele O "Cloud Computing Security Issues and Challenges".

v. Traian Andrei, "Cloud Computing Challenges and Related Security Issues".

vi. Ahmed E. Youssef, "Exploring Cloud Computing Services and Applications ".

vii. William Allen,"Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions".

viii. " https://en.wikipedia.org/wiki/Denial-of-service_attack", Tuesday, November 14, 2017, 1:31pm.

ix. "http://www.thewindowsclub.com/dos-denial-of-service-attack", Tuesday, November 14, 2017, 9:15pm.

x. Rashmi, Dr.G.Sahoo&Dr.S.Mehfuz, "Securing Software as a Service Model of Cloud Computing: Issues and Solutions".

xi. SandeepMukherji&ShashwatSrivastava" Pros and Cons of Cloud Computing Technology".

xii. Daniel Hallmans, "Challenges and opportunities when introducing cloud computing into embedded systems ".

xiii. Mohammed Humayun Kabir, Syful Islam, Md. Javed Hossain & Sazzad Hossain, "A Detail Overview of Cloud Computing with its Opportunities and Obstacles in Developing Countries".

xiv. T. Vaikunth Paiand Dr. P. S. Aithal, "Cloud Computing Security Issues - Challenges and Opportunities".

xv. R.Arokia Paul Rajan, S. Shanmugapriyaa, "Evolution of Cloud Storage as Cloud Computing Infrastructure Service".

xvi. Maria Evans, Tam Huynh, aria Evans&Mark Singh, "Cloud Storage".

xvii. "https://cloud.google.com/files/CloudStorage", Thursday, November 21, 2017, 11:30pm.

xviii. John McCarthy, "Architects of the Information Society, Thirty-Five Years of the Laboratory for Computer Science at MIT".

xix. Amy Schurr, "Keep an eye on Cloud Computing".

xx. "www.dialogic.com/Introduction to cloud computing", Thursday, February 22, 2018, 11:19pm.

xxi. " https://www.ibm.com/blogs/cloud-computing/2014/03/a-brief-history-of-cloud-computing-3/", Thursday, February 22, 2018, 11:45pm.

xxii. "https://www.linkedin.com/pulse/five-essential-characteristics-cloud-computing-sankar-somepalle", Thursday, February 22, 2018, 11:51pm.

xxiii. "http://focus.forsythe.com/articles/559/The-Top-3-Cloud-Computing-Service-Models", Thursday, February 22, 2018, 12:00am.

xxiv. Cloud Computing Security Issues, Challenges and Solution, Pradeep Kumar Tiwari, Dr. Bharat Mishra.

xxv. Data Security Challenges and Its Solutions in Cloud Computing, R.VelumadhavaRaoa, K. Selvamanib.

xxvi. " https://www.cdnetworks.com/en/news/cloud-security--public-vs.-private-cloud/4210", Monday13, 2018, 11:00am.

xxvii. "https://www.salesforce.com/hub/technology/benefits-of-cloud/",Monday13, 2018, 11:30am.