Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

New Security Paradigm in Cloud Computing

[1]Rishabh Bhardwaj, [2]Ratish Agarwal, [3]Sachin Goyal, [4]Mahesh Pawar
[1]Cyber law& Information Security, NLIU, Bhopal, Madhya Pradesh, India
[2, 3, 4] Information Technology, RGPV, Bhopal, Madhya Pradesh, India

Abstract: Nowadays, with evolution of the new technology cloud computing play a vital role for the business organization. Cloud computing provides the ability to utilize scalable, distributed environment via internet on demand and pay as per use. Today's cloud computing place centralized, universal trust in all the cloud nodes. However there may be negative impact on the nodes that are compromised and leads to various attacks. To address these issues, a number of research papers have been presented by authors. In this paper are given a review of these papers. More precisely are try to find out the limitation of existing technique and try to overcome them.

Key words: cloud computing, penny, silver lining, decentralised, security.

I. Introduction

Nowadays a new technology is being implemented for the welfare of the people that makes sure that all the people are using this technology more conveniently. Cloud computing is one of the most dominating technique that influences the people and large organization to use this technology. Cloud computing provides the ability to utilize scalable, distributed environment via internet. Cloud computing is tremendously growing providing wide range of business sector in its organization. This business concept was remunerative to many organizations reason being why many big organizations show their interests in this field. They take several steps to enhance their business to reach public at large scale.

By the year 2014, very few of the known organizations provide their cloud facility to the every user. Microsoft sky drive has been providing about 25Gb space, Google drive provides about 15 GB space, and similarly icloud and drop box also provide 5GB, 2GB space respectively[13], to the user to store their critical data in this provided area. But the security is one of the major factors that hamper the growth of this technology.

A. Evolution of cloud computing

This cloud computing technology is not new one, it has been used from an incunabula. The trend toward cloud computing was started at very early stages, at that time it was used with the concept of mainframe and then it moved to the distributed computing that is grid computing. The grid computing provides virtual pools of computation resources but it was different from cloud computing. For the very first time a large number of the systems were applied to the single problem, usually scientific in nature and it requires exceptionally high levels of parallel computation. In grid computing the main focus is on the work load of location needed computing resources, which was remote and readily available to the user. Usually, a large task was divided into the smaller task sections to run it parallel in the cluster of grid computing and it is viewed as just one virtual server. And this was usually utilized by the bigger organization.
Basically it was evolved in three phases:-

Phase 1:- Mainframe computing
In this phase, all the critical information or data of the organization was stored at one physical location and ran all software application. It easily supported multiple applications through one mainframe, maintaining such a large piece of hardware was expensive and inefficient.

Phase 2:- Distributed computing
The mainframe computing was less effective that is why; distributed computing came in use as it was comparatively easy to manage. Here business replaces the mainframe into the distributed computing where multiple systems used and each system has an enough capable space to store the data and run application. But the only problem that came up was that; the computers were not coordinated with each other and it was difficult to share the data moreover every resource saved was negated because every computer changed, even fixing or updating didn't helped. Hence, next phase was introduced namely 'cloud computing'.

Phase 3:- Cloud Computing
Nowadays, cloud computing is widely used. Here cloud shares network of computer by which people and company store data and run software. In this all the people and different organizations are free to use it according to their requirement and utility managing it according to their choice.

Cloud computing offer the central management and coordination of the main frame with the affordable scalability of the distributed computing. It is the best solution for all the people, large and small organization.

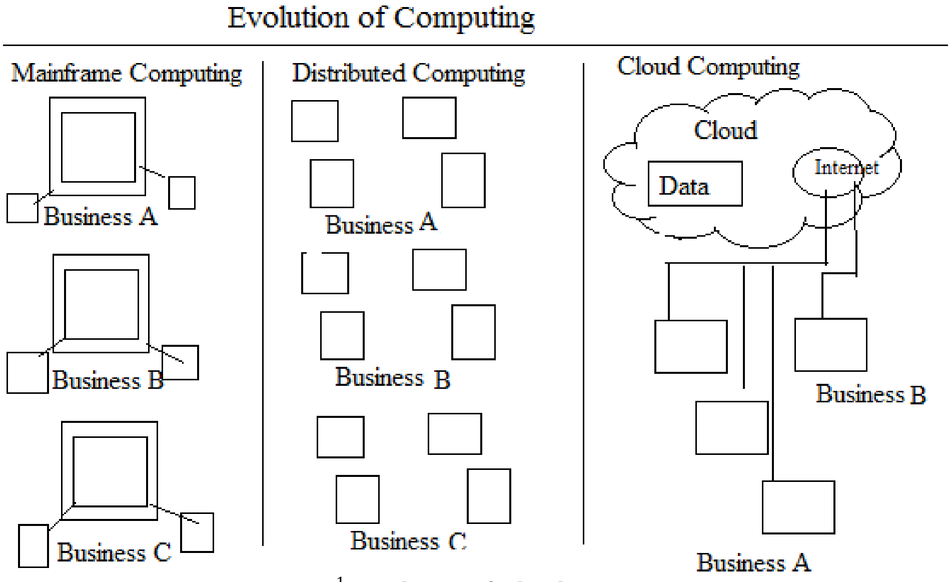

Figure-1[1]: Evolution of Cloud Computing

B. *What is cloud computing?*

In the year 2009, National Institute of Standard Technology (NIST) information technology defined cloud computing[2], "cloud computing is the model for enabling convenient, on-demand network access to the shared pool of configuration and reliable resources computing resources that can be rapidly provisioned and released with minimal management effort or services provider interaction".

The cloud computing comprises of the three services model, four deployment model and five essential characteristics.

The three services models are as follows:-

1) **Cloud software as a services (SaaS):-** In the SaaS, specific-purpose software was provided by the vendor to the customer over a network via internet.

2) **Cloud platform as a services (PaaS):-** In the PaaS, it offers high level integrated environment to build, test, and deploy custom applications. Here the developer accepted some restriction on the type of the software that was used to build in application scalable.

3) **Cloud infrastructure as a services (IaaS):-** In this, it provided hardware, various software and equipment to deliver software application with a resource usage based pricing model.

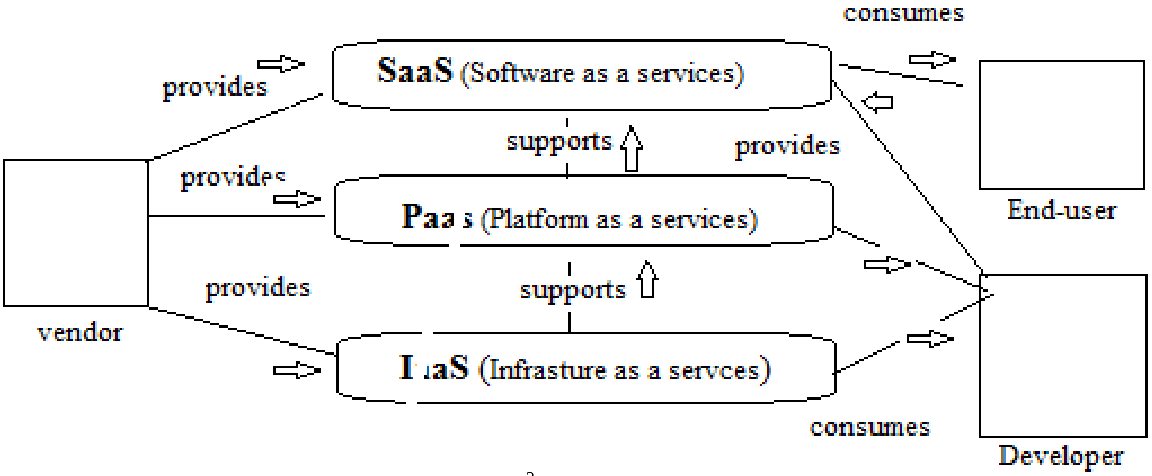
consumes
provides
SaaS (Software as a services)
supports
provides
provides
PaaS (Platform as a services)
End-user
provides
supports
vendor
IaaS (Infrastruce as a servces)
consumes
Developer

Figure-2[3]: Services Model

All these level were used to reduce the expenditure and infrastructure. In every service model vendor provide a various services to the customer, the three services models are infrastructure as a service, platform as a services and software as a services.

[1] http://www.datahouse.com/assets/files/Cloud-1.0.pdf, visited on 10/1/2015

[2] John W, rittinghouse and james F. ransome, et al, "cloud Computing Implementation, Management and Security" , CRC Press Taylor and Francis Group, 2010.

[3] http://blog.ascens-ist.eu/category/clouds/, visited on 11-1-2015

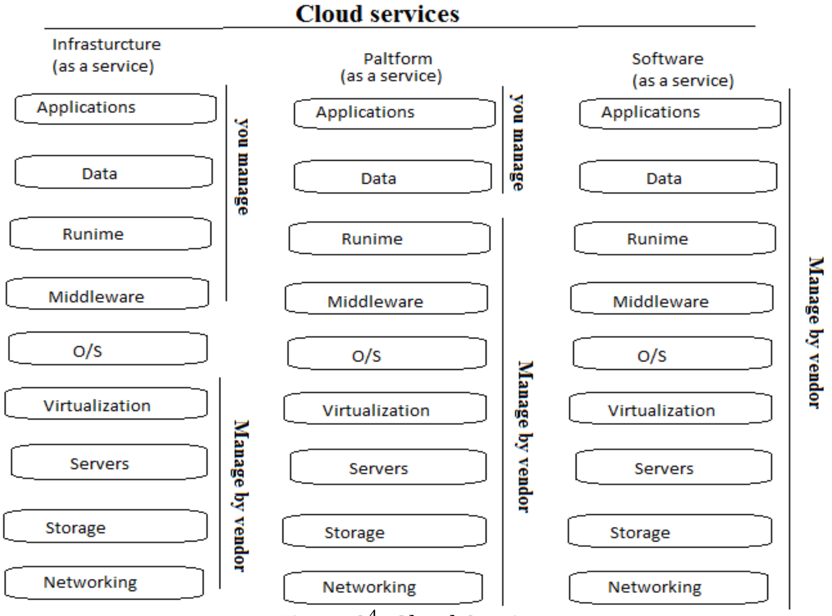

Figure-3[4]: Cloud Services

In this way some of the services were managed by the vendor. All the services were managed by the customer in software as services by customer, in platform as a services application and data was managed by the customer, rest of the services were managed by the vendor, in infrastructure as a services application, data, run time, middleware and OS were managed by the customer and rest were managed by the vendor in this way all the services are fulfilled by the vendor to the customer

The four deployment models of cloud computing are:-

1) Private cloud: - The private cloud infrastructure has been used or managed by an individual organization or the third party and may exist on the premises or off premises.

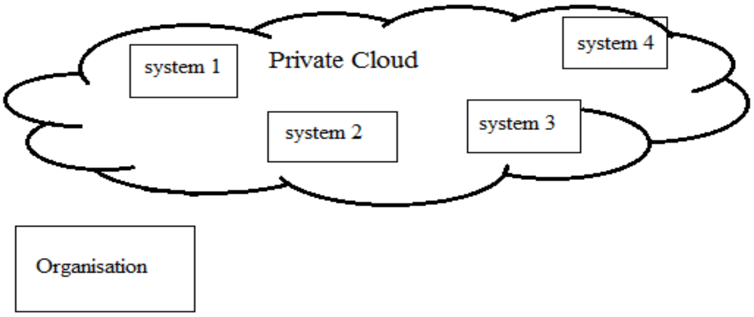

Figure-4[5]: Private Cloud

2) Community cloud: - In this the cloud infrastructure was shared by the several organization or specific community. It is managed by the organization or the third party and may exist on the premises or off premises.

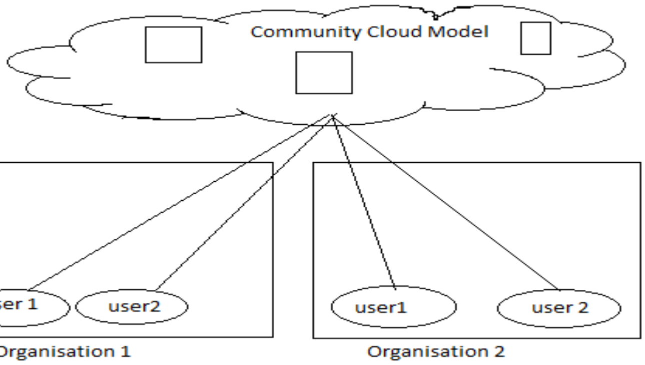

Figure-5[6]: Community Cloud

[4] http://www.datahouse.com/assets/files/Cloud-1.0.pdf, visited on 11-1-2015

[5] http://www.falconitservices.com/IT%20Services%20Miami/Private%20Cloud%20Infrastructure.aspx, visited on 11-1-2015

[6] http://www.tutorialspoint.com/cloud_computing/cloud_computing_community_cloud_model.htm, visited on 11-1-2015

3) **Public cloud**: - This cloud infrastructure is being available to all the users.

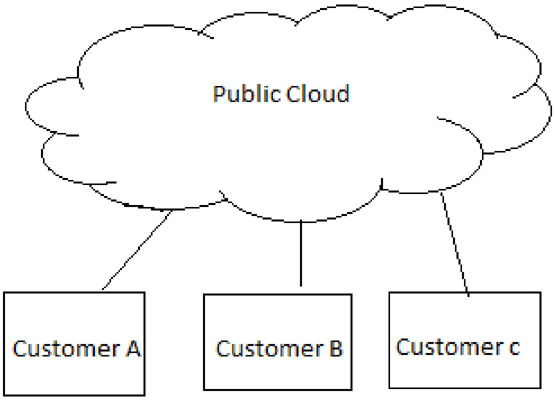

Figure-6[7]: Public Cloud

4) **Hybrid cloud**: - Here the cloud infrastructure is a composition for more than one cloud (private, public, community); they are bound together by the standard or preparatory technology that enables data application portability.

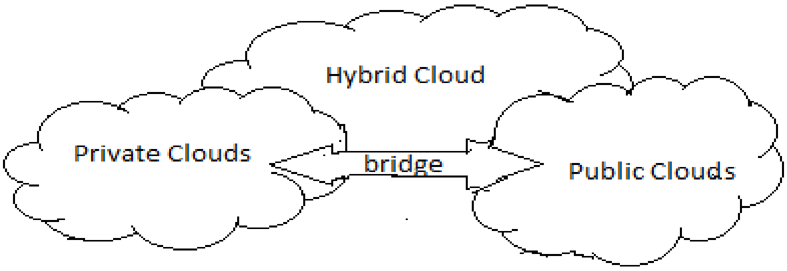

Figure-7[8]: Hybrid Cloud

The five essential characteristics are as follows:-

1. **On-demand self-services**:- In this an on demand self services, it provide customer to use cloud computing without any human interaction between the customer and cloud services provider. In this the customer can schedule their use of the cloud services (i.e. computation and storage as needed) in addition to managing and deploying these services.

2. **Resources pooling**: - Here in cloud there is a scalable and flexible resources pool according to the needs of the customer and these resources were allocated efficiently for optimum performance.

3. **Location independence**:- This is a most important characteristic which was used by the customer that is location independence because here the customer can use the cloud services when it want to used it without any intervention. Whenever, customer wants to use their service which was independent of the area.

4. **Rapid elasticity**: - Rapid elasticity shows the ability of the cloud to expand or reduce allocated resources quickly and efficiently to meet the requirements of the self-service characteristics of the cloud computing.

5. **Measured services**: - In measured services customer can be billed on the bases of the utilization of the cloud resources which was allotted for the particular session. Resources usage can be monitored controlled and reported providing transparency for both the provider and customer of the utilized services.

II. REVIEW OF LITERATURE

The number of the paper was published by the author in this area. Some important contributions are given below:-

In [1], Safwan Mahmud Khan, et al. have discussed about the decentralized trust in new security paradigm in cloud computing. This paper was discussed about data computation integrity and security are the main concern in the cloud computing. Nowadays the cloud computing was used in the centralized way and has a trust on all the nodes of the cloud but there is a negative consequences that if any one of the node was compromised or find any vulnerability in the cloud than it lead to myraid attacks. That’s why to address this weakness this paper was published in this paper it self that purposed various algorithms and models to mitigate that risk.

First of all they proposed Hatman algorithm which is based on the decentralized trust and it used to ensure computation integrity. This Hatman was deployed reputation based trust management system for Hadoop cloud. The second proposed work is anonymous cloud decentralization trust by billing information from submitted jobs and it is used to overcome the various problems that are privacy preserving computing and data ownership in the cloud which is identified by the IP address. Third proposed work is penny, it is also based on the fully decentralized per-to-per structure and it is used to support integrity and confidentiality of the data on information, it also ensure the ownership privacy that permits peer to published data with out divulging the ownership of the data.

[7] http://blog.pluralsight.com/private-vs-public-cloud, visited on 11-1-2015

[8] http://blog.p3infotech.in/2013/hybrid-cloud-model/, visited on 11-1-2015

Another proposed work is the cloud cover decentralization trust on user sides and it also proposed new form of the security as a service (SECaas) to provide trust in the serial computing in the untrusted environment. At last silver lining is the last proposed work that is in-line information flow tracking code into the untrusted job binaries and also it provide custom security policy without any change in the kernel of the cloud, operating system hypervisor and file system implementation.

In [2], Ahmed Shawish and Maria Salama, et al. have discussed about the cloud computing paradigm and technology. It is the cloud computing paradigm which is used for the managing and delivers of the services on the cloud through the internet. This paper was concluding about the cloud anatomy, definition, characteristics and core technology. This chapter also addresses the customer-related aspect such as services level management, services cost and security issues. Finally, it covers detail comparison between cloud computing paradigm and other which is related to the significant challenges.

In [3], Kevin hamlen, Murat kantarcioglu, Latifur khan and Bhavani thuraisingham, et al. this work is also support by the AFOSR project on secure information grid. This paper was discussed about the various security issues in cloud computing which was include storage security, data security, network security and secure virtualization. This paper was discussed on secure federation query processing with MapReduce, hadoop and the use of the co-processors for cloud computing. A major aspect of the cloud computing was building trust application from untrusted component.

In [4], Mumtum Zico Meetei and Anita Goel, et al. have discussed about the security issues in the cloud computing. Security is one of the key factor which hampered the growth of cloud computing. There are some of the security challenges that are data storage security, data transmission security application security and security related to the third-party resources. This paper was discussed about the various security issues arising from the usage of the cloud services.

In [5], John W, rittinghouse and James F. ransome, et al, have discussed about the cloud computing implementation, management and security. Basically this book tell about the basic of the cloud computing and also cover various security issues that was arises in the cloud computing. Nowadays many organizations used a centralized cloud where the large amount of data was stored, while preserving user privacy, security, identity and their application-specific arises many concern about data protection and this concern lead to many question about the legal framework that should be for cloud computing environments. Today’s cloud computing is major concern for many big organization.

In [6], Rajesh Piplode and Umesh Kumar Singh, et al. was discussed about an overview and the study of cloud computing. Cloud computing is the most promising technology to facilitate the development of large scale, on-demand, flexible computing infrastructure. But without security embedded in to this technology all the data was stored in the single box that is it is easier for the hacker to attack on the cloud and get critical data. This paper also include several security and challenging issues, immerging application and the future trend of the cloud computing. The trend of adopting this technology by the organization automatically introduces new risk over the exiting risk.

In [7], Vahid Ashktorab and Seyed Reza Taghizadeh, et al. was discussed about security threads and countermeasure in cloud computing. This paper was about various security threads of cloud computing system, which measuring the countermeasure which was faced by the different organization at present. This paper also addressing various issues requires confidence from user for the cloud application and its services. This paper also provide little known list of threads and also categorized these threads according to different view points.

In [8], Deyan Chen and Hong Zhao, et al. was discussed about the data security and privacy protection issues in the cloud computing. According to this paper some business critical-application, large business organization, especially large enterprises would not move to the cloud because of the privacy and security issues. This paper provide abridged but all around analysis on data security and privacy protection issues associated with all stage of the data life cycle and also discussed about the current solution. This paper also deal with the future research work for the cloud computing.

In [9], Kuyoro.s.o, Ibikunle F. and Awodele O., et al. was discussed about the security issues and challenges in cloud computing. Usually cloud computing services are provided by the third part who owns the cloud infrastructure it advantage to mention but a few include scalable, resilience, flexibility, efficiency and outsourcer’s non-core activity. Basically many organizations are not accepting cloud services because of the security and privacy issues, such that the customer needs to be vigilante understanding the risk of the data breaches in the new environment. Cloud was hampered because of the issues arises in security. This paper introduced a detail analysis of the cloud computing security issues and challenges focusing on the cloud computing types and service deliver types.

In [10], AllanA.Friedman and Darrell M. west, et al. was discussed about the security about the privacy and security on the cloud. This paper was established a set of concern about the cloud and highlight what is new and what is not. It also analyzes a set of policy issues that represent systematic concern deserving attention of policy makers. In this paper also find out that Human factor and surrounding institute is the weakest link in the security in the cloud. Cloud computing has the potential to generate innovation without sacrificing privacy and security.

In [11], Meiko Jensen and Nils Gruschka, et al. was discussed was about the technical security issues in cloud computing. It was basically deals with the security and trust issues when the data was stored by the user in the cloud and it leaves the protection sphere of the data protection. This paper was focused about the usage of the cloud services and it was done by the underlying technology which was used to build these cross domain internet connected collaboration.

In [12], Preadeep Kumar Tiwari and Dr. Bharat Mishra, et al. was discussed about the Cloud computing security issues, challenges and solution. Cloud used as distributed resources in open environment that’s why it is important to provide security and trust to share the data for cloud application. This paper was show about the successful implementation of the cloud in the enterprise with proper risk countermeasure and threads. This paper also explain about the solution that how to secure the cloud security, privacy and reliability when the third party is processing sensitive data. It also explains cloud computing strength, weakness with application risk management and also told about the advantage and disadvantage of the cloud.

III. PROPOSED METHODOLOGY

Nowadays cloud is one of the new trends in the technological era. Many large organization are using this technology because it provide large storage to the information in the cloud as well as it is also open to the people to use it, numerous organization provide this services to the people like, Microsoft sky drive provide about 25Gb space, Google drive provide about 15 GB space, similarly icloud and drop box also provide 5GB, 2GB space respectively to the user to store their critical data in this provided area.

But there is major problem that is privacy and security which is the wide concern in the cloud. Several steps were taken by them to mitigate the risk and to overcome the problem of privacy. First of all steps, were taken to provide the security on the server side and maintain the integrity and confidentiality of the information or the data. Here all the data or information were stored in the centralized way which is also the major concern because if one node is compromised then the whole data is at risk that is why several model or steps were taken to mitigate the risk.

This paper examines most of the issues for the perspective of the trust decentralization, minimization and management in the cloud. Here the full paper explores the problems in the trust management of the cloud.

The very first is to understand the working of penny [1] which is based on the peer-to-peer topology and it is used to eliminate the centralized trust. All the master nodes can act as peer and the jobs and data are distributed between them. Peer-to-peer networking is distributed, load balancing cloud computing paradigm which share work load between the peers. Penny is fully distributed reputation management system which is based on the Eigen trust to surely manage data label without central authority that is why it is used to maintain integrity, confidentiality and ownership of the data. To protect the data ownership, penny employs a cryptographic protection. However, there is a problem that is; various attacks like denial of services, message misrepresentation and to mitigate the effect of this attacks various securities were deployed.

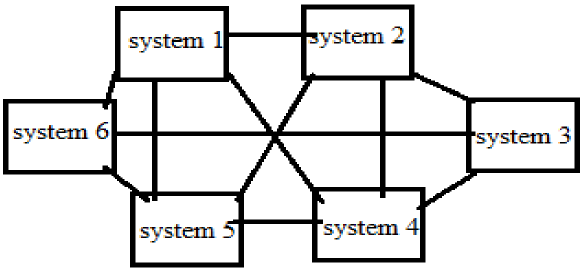

Figure9[9]: Peer-to-peer network

To mitigate the *DOS* attack by using *API* which is based on Oauth-2 model. Oauth-2 is authorization framework that allows most of the application to obtain limited access to the user account which is based on https services. Initially, user is needed to fulfil the queries and provide all the detail required to register into the resource owner. After registration into the resource owner will grant access to the user. In the next step user now request for the token to the service server, in response to which service server will provide security token, which now user will get verified by sending to the 2nd server i.e., authorized server, that will granted authentication to the user, and therefore now the user is connected to server and ready to access it.

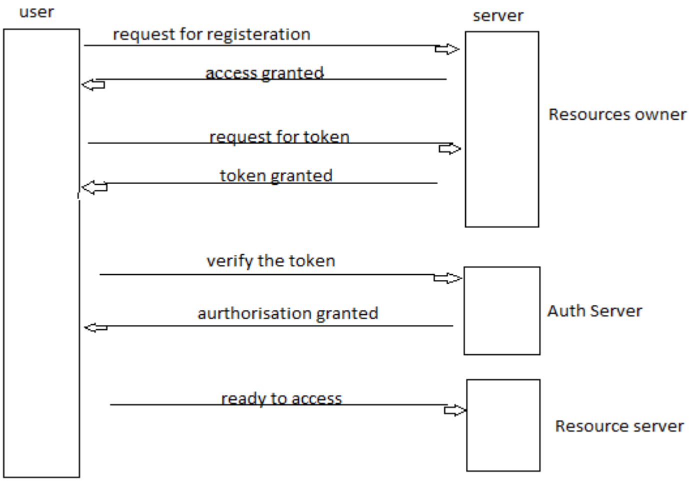

Figure 10: Mitigate *DOS* attack

[9] http://www.springer.com/cda/content/document/cda_downloaddocument/PPNA_CfP_P2P+Cloud+Systems.pdf?SGWID=0-0-45-1337127-0, visited on 9-2-2015

Silver line [1] is one of the in-line information flow tracking code into the untrusted job binaries and also it provide custom security policy without any change in the kernel of the cloud, operating system hypervisor and file system implementation. In silver line security implementation was completely separate and orthogonal. Different cloud provider has different internal architecture, but in general there is some level of topologies which consist of a few master nodes and large number of the slaves node. The complexity in the data dependency and jobs which leads to various attacks that might violate the user information flow which motivate to put some strong and flexible approach to some policies. Addressing the confidentiality bella-laPadulla was deployed. Our proposed work on silver lining is that to gain the confidentiality and integrity in the cloud by Appling mandatory access control policies with Clark-Wilson model.

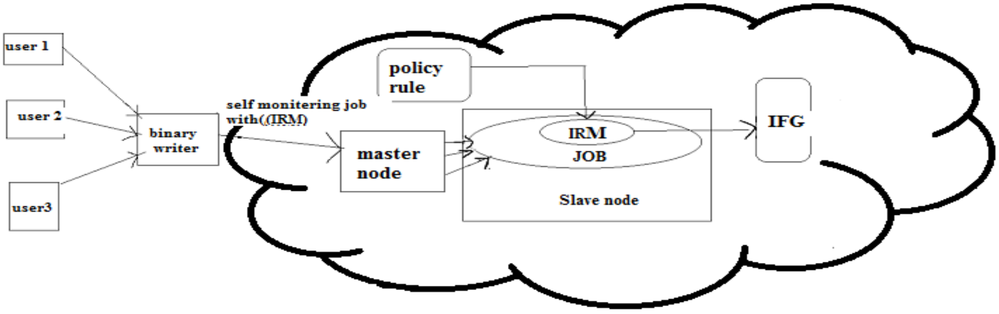

Figure 10: system architecture in silver lining

The Clark Wilson model is based on the integrity, where the user cannot access and manipulate the object directly, but must access the object through program. There are three major goal of integrity such as prevent unauthorized user for making modification, prevent authorized user from making improper modification and maintain internal and external consistency

IV. CONCLUSIONS

Cloud is seemed to be new phenomenon which is set to be revolutionary by the way internet was use, but there is much to be caution about. The new technologies were emerging at rapid rate, each with a technological advancement and the potential of making human lives easier. However in the cloud there are many issues. This research paper was addressing many problems that were occurring in the penny cloud and silver lining of the cloud, so that to enhance the utility of the cloud.

REFERENCES

[1] Safwan Mahmud Khan, et al. "decentralized trust: new security paradigm in cloud computing" (USA: 2013)

[2] Ahmed Shawish and Maria Salama, et al "Cloud Computing: Paradigm and Technology"

[3] Kevin hamlen, Murat kantarcioglu, Latifur khan and Bhavani thuraisingham, et al. "Security Issues For Cloud computing" (USA:2010)

[4] Mumtum Zico Meetei and Anita Goel, et al. "Security Issues in Cloud Computing".

[5] John W, rittinghouse and james F. ransome, et al, "cloud Computing Implementation, Management and Security" , CRC Press Taylor and Francis Group, 2010.

[6] Rajesh Piplode and Umesh Kumar Singh, et al "An Overview and Study Security Issues and Challenges in cloud computing", International Journal of Advanced Research in computer science and Software Engineering" volume 2, Issue 9, September 2012, ISSN 2277-128X.

[7] Vahid Ashktorab and Seyed Reza Taghizadeh, et al. "Security threads and countermeasure in cloud computing", International Journal of application or Innovation in Engineering and Management, volume 1, Issue 2, October 2012, ISSN 2319-4847.

[8] Deyan Chen and Hong Zhao, et al. "Data Security and Privacy Protection Issue in Cloud Computing" International Conference on Computer Science and Electronic Engineering,(2012)

[9] AllanA.Friedman and Darrell M. west, et al "Privacy and Security in Cloud Computing" (2010)

[10] Kuyoro.s.o, Ibikunle F. and Awodele O., et al "Cloud Computing Security Issues and Challenges"

[11] Meiko Jensen and Nils Gruschka, et al. "The Technical Security Issues in Cloud Computing"

[12] Meiko Jensen and Nils Gruschka, et al. "Cloud Computing Security Issues, Challenges and Solution" International Journal of Emerging Technology And Advanced Engineering, volume 2, Issue 8, August 2008, ISSN 2250-2459.

[13] http://www.digitaltrends.com/mobile.can-apple-icloud-compete-after-dropping-free-storage-limit/, visited on 23/2/2015.