Migration from Single-Cloud to Multi-Cloud Computing

J Suresh Babu, K Kishore, K E Naresh Kumar
[II-M.Tech]-CSE, Asst.Profin CSE Dept.,DrKVSRIT Kurnool, Asst Prof in CSE Dept., RGMCET Nandyal.

Abstract

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Ensuring the security of cloud computing is a major factor in the cloud computing environment, as users often store sensitive information with cloud storage providers but these providers may be untrusted.

Dealing with "single cloud" providers is predicted to become less popular with customers due to risks of service availability failure and the possibility of malicious insiders in the single cloud. A movement towards "multi-clouds", or in other words, "inter clouds" or "cloud-of-clouds" has emerged recently.

This paper surveys recent research related to single and multi-cloud security and addresses possible solutions. It is found that the research into the use of multi-cloud providers to maintain security has received less attention from the research community than has the use of single clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

Key Words: Component, formatting, style, styling, insert.

1. Introduction

The use of cloud computing has increased rapidly in many organizations. Small and medium companies use cloud computing services for various reasons, including because these services provide fast access to their applications and reduce their infrastructure costs. Cloud providers should address privacy and security issues as a matter of high and urgent priority. Dealing with "single cloud" providers is becoming less popular with customers due to potential problems such as service availability failure and the possibility that there are malicious insiders in the single cloud. In recent years, there has been a move towards "multi-clouds", "inter-cloud" or "cloud-of-clouds".

The main focused on the issues related to the data security aspect of cloud computing. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider. Protecting private and important information, such as credit card details or a patient's medical records from attackers or malicious insiders is of critical importance. In addition, the potential for migration from a single cloud to a multi-cloud environment is examined and research related to security issues in single and multi-clouds in cloud computing is surveyed.

A. Background

NIST describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

NIST describes cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". Cloud providers should address privacy and security issues as a matter of high and urgent priority.

Cloud Computing appears as a computational model or paradigm and its main objective is to provide secure, quick, convenient data storage and net computing service, with all computing resources being visualized as services and delivered over the Internet. Cloud enhances collaboration, agility, scaling, and availability, the ability to scale to fluctuations in demand, as well as the acceleration of development work and provides the potential for cost reduction through optimized and efficient computing.

Cloud computing combines a number of computing concepts and technologies such as SOA, Web 2.0, virtualization and other technologies with reliance on the Internet, providing common business applications online through web browsers to satisfy the computing needs of users, while the software and data are stored on the servers. There is commercial pressure on businesses to adopt Cloud

computing models but customers need to ensure that their cloud services are driven by their own business needs rather than by providers' interests, which are driven by short-term revenues and sales targets together with long-term market share aspirations.

The global presence of the Internet and the introduction of wireless networking and mobile devices featuring always on Internet connectivity have raised expectations of users and demand for services over the internet. However, the architectures required by service providers to enable Web 2.0 has created an IT service that is differentiated by resilience, scalability, reusability, interoperability, security and open platform development. This has effectively become the backbone of Cloud computing and is considered by a number of vendors and services to be an operating system layer of its own.

The importance of Cloud computing is increasing and it is receiving growing attention in the scientific community. In fact, a study of Gartner has considered Cloud Computing to be the first technology among the top 10 technologies, extremely important and with the best prospect in 2011 and successive years for companies and organizations.

NIST defines Cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Between the essential characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, highly abstracted resources, near instant scalability and flexibility and measured service. The three service models are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Finally, the four deployments models are private cloud, community cloud, public cloud and hybrid cloud.

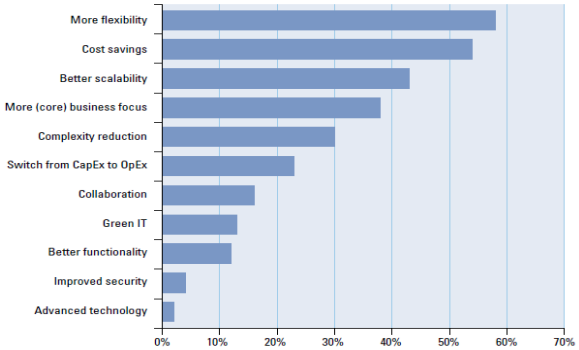

Figure 1. Benefits of Cloud computing

In another study about Cloud computing the majority of the participants expect three main drivers of Cloud computing (see Figure 1): more flexibility, followed by cost savings and better scalability of their IT. Cloud computing can bring relief by the faster deployment of applications for less cost. In this same study, an overwhelming majority of participants consider security issues to be their main concern regarding the use of Cloud computing. In addition, legal, privacy and compliance issues are considered to be areas of risks. Focusing on the security issue, the majority of participants agree that security concerns are blocking their move to the cloud. It appears that they are not worried primarily about the lack of security measures in themselves, but about the lack of transparency on the side of vendors.

The ENISA report highlights the benefits that some small and medium size companies can realize with Cloud computing. A smaller, cost-constrained organization may find that a cloud deployment allows them to take advantage of large-scale infrastructure security measures that they could not otherwise afford. Some of the possible advantages include DDOS (distributed denial of service) protection, forensic image support, logging infrastructure, timely patch and update support, scaling resilience, and perimeter protection (firewalls, intrusion detection and prevention services).

2. CLOUD COMPUTNG MODELS

A. Public Cloud

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

The main benefits of using a public cloud service are:

1. Easy and inexpensive set-up because hardware, application and bandwidth costs are covered by the provider. Scalability to meet needs.
2. No wasted resources because you pay for what you use.
3. The term "public cloud" arose to differentiate between the standard model and the private cloud, which is a proprietary network or data center that uses cloud computing technologies, such as virtualization. A private cloud is managed by the organization it serves. A third model, the hybrid cloud, is maintained by both internal and external providers. Examples of public clouds include Amazon Elastic Compute Cloud (EC2), IBM's Blue Cloud, Sun Cloud, Google AppEngine and Windows Azure Services Platform.

B. Community Cloud

Private cloud (also called internal cloud or corporate cloud) is a marketing term for a proprietary computing architecture that provides hosted services to a limited number of people behind a firewall. Advances in virtualization and distributed computing have allowed corporate network and datacenter administrators to effectively become service providers that meet the needs of their "customers" within the corporation. Marketing media that uses the words "private cloud" is designed to appeal to an organization that needs or wants more control over their data than they can get by using a third-party hosted service such as Amazon's Elastic Compute Cloud (EC2) or Simple Storage Service (S3).

C. Hybrid Cloud

A hybrid cloud is a Cloud Computing environment in which an organization provides and manages some resources in-house and has others provided externally. For example, an organization might use a public cloud service, such as Amazon Simple Storage Service (Amazon S3) for archived data but continue to maintain in-house storage for operational customer data. Ideally, the hybrid approach allows a business to take advantage of the scalability and cost-effectiveness that a public cloud computing environment offers without exposing mission-critical applications and data to third-party vulnerabilities.

D. Private Cloud

A community cloud may be established where several organizations have similar requirements and seek to share infrastructure so as to realize some of the benefits of cloud computing. With the costs spread over fewer users than a public cloud (but more than a single tenant) this option is more expensive but may offer a higher level of privacy, security and/or policy compliance. Examples of community cloud include Google's "Gov Cloud".

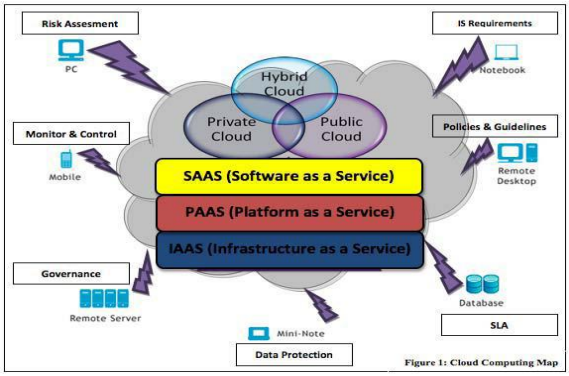

Fig. 2 Cloud Computing Models

3. All Cloud Models Are Not The Same

Although the term Cloud Computing is widely used, it is important to note that all Cloud Models are not the same. As such, it is critical that organizations don't apply a broad brush one-size fits all approach to security across all models. Cloud Models can be segmented into Software as a Service (Saas), Platform as a service (PaaS) and Integration as a Service (IaaS). When an organization is considering Cloud Security it should consider both the differences and similarities between these three segments of Cloud Models:

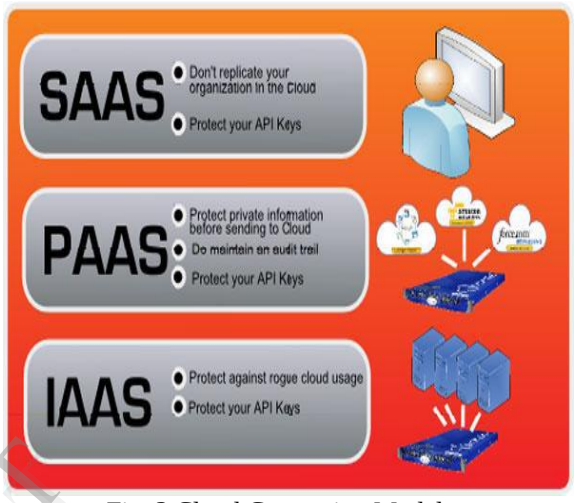

Fig. 3 Cloud Computing Models

4. SECURITY ISSUES AND CHALLENGES:

Cloud computing is a emerging technology with shared resources, lower cost and rely on pay per use according to the user demand. Due to many characteristics it has effect on IT budget and also impact on security, privacy and security issues .In this section all these issues are discussed. All those CSPs who wish to enjoy this new trend should take care of these problems. It is developing country with no any proper IT strategy, a CSP should give their full attention to security aspect of cloud because it is a shared pool of resources. Customer not know where the data are stored, who manage data and other vulnerabilities that can occur. Following are some issues that can be faced by CSP while implementing cloud services.

4.1 Privacy Issue

It is the human right to secure his private and sensitive information. In cloud context privacy occur according to the cloud deployment model. In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the dominant architecture when cost reduction is concerned, but relying on a CSP to manage and hold customer information raises many privacy concerns and are discussed under:

4.1.1 Lack of user control

In SAAS environment service provider is responsible to control data. Now how customer can

retain its control on data when information is processed or stored. It is legal requirement of him and also to make trust between customer and vendor. In this new paradigm user sensitive information and data is processed in 'the cloud' on systems having no any, therefore they have danger of misuse, theft or illegal resale. Adding more, this is not patent that it will be possible for a CSP to guarantee that a data subject can get access to all his/her PII, or to comply with a request for deletion of all his/her data. This can be difficult to get data back from the cloud, and avoid vendor lock-in.

4.1.2 Unauthorized Secondary Usage

One of the threats can occur if information is placed for illegal uses. Cloud computing standard business model tells that the service provider can achieve profits from authorized secondary uses of users' data, mostly the targeting of commercials. Now-a-days there are no technological barriers for secondary uses. In addition, it has the connected issue of financial flexibility of the CSPs: for example, possibility of vendor termination, and if cloud computing provider is bankrupted or another company get data then what would happen.

4.1.3 Trans border Data Flow and Data Proliferation

One of the attribute of cloud is Data proliferation and which involves several companies and is not controlled and managed by the data owners. Vendor guarantee to the ease of use by copy data in several datacenters. This is very difficult to ensure that duplicate of the data or its backups are not stored or processed in a certain authority, all these copies of data are deleted if such a request is made.

4.1.4 Dynamic provision

Cloud has vibrant nature so there is no clear aspect that which one is legally responsible to ensure privacy of sensitive data put by customer on cloud.

4.2 Security

Public cloud not only increases the privacy issue but also security concern. Some security concerns are described below:

4.2.1 Access

It has the threat of access sensitive information. The risk of data theft from machine has more chances in cloud environment data stored in cloud a long time duration any hacker can access this data.

4.2.2 Control over data lifecycle

To ensure the customer that it has control over data, if it remove or delete data vendor cannot regain this data. In cloud IAAS and PAAS models virtual machine are used that process and then media wiped but still there is no surety that next user cannot get that data.

4.2.3 Availability and backup

There is no any surety of availability and back up of data in this environment. In business backup is one of the important consideration.

4.2.4 Multi-tenancy

It is feature of SAAS that one program can run to multiple machines. CSP use multi-tenant application of cloud to reduce cost by using virtual machine but it increase more vulnerability.

4.2.5 Audit

To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction without effecting integrity.

4.3 Trust

Trust is very necessary aspect in business. Still cloud is fail to make trust between customer and provider. So the vendor uses this marvelous application should make trust.Weak trust relationship and lack of customer trust cause many problems during deployment of cloud services.

4.4 Mitigation Steps

This section includes mitigation steps and some solution to overcome the issues discussed in previous section. It provides guidelines to the companies that offer cloud services .It will helpful to them to make proper strategy before implementing cloud services. There are some alleviations to reduce the effect of security, trust and privacy issue in cloud environment. There are many adoption issues like user get privilege to control data cause low transaction performance, companies are worried from cyber-crimes and the Internet speed also effect the performance, virtual machines are taking milliseconds to encrypt data which is not sufficient and to avoid risk there is contract between parties to access data. So mitigate such type of problems some action should take place. Some steps are listed below:

- Build up an iterative policy for relocation from traditional environment to Cloud environment.
- As this upcoming trend reduce cost but be careful to select possible solutions to avoid problems in this computing and calculate the effect on the system just not consider the outlay.
- Providers should be aware regarding new changes and assure that customer's access privileges are limited.
- Cloud is a shared pool of resource. Discover the linked service providers that wants to connected to particular Cloud service provider to query, which provider has right to use facts and data .
- System for monitoring should be request for exclusion
- Service provider should tell customer for managing polices for security beside

provider's owned policies, with in the duration of services.

- Make it sure, that the data being transferred is protected and secured by standard security techniques and managed by appropriate professionals.

4.5 Proposed Solutions

The Table 3 shown below gives a look on the solutions that are helpful to the cloud customer and companies offer services with secure and trusty environment.

Table 1: Solutions

Solution	Description
Data Handling Mechanism	Classify the confidential Data. Define the geographical region of data. Define policies for data destruction.
Data Security Mitigation	Encrypting personal data. Avoid putting sensitive data in cloud.
Design for Policy	Fair information principles are applicable.
Standardization	CSP should follow standardization in data tracking and handling.
Accountability	For businesses having data lost, leakage or privacy violation is catastrophic Accountability needs in legal and technical.Audit is need in every step to increase trust All CSP make contractual agreements.
Mechanism for rising trust	Social and technological method to raise trust. Joining individual personal rights, preferences and conditions straightforwardly to uniqueness of data. Devices connected should be under control by CSP. Use intelligent software.

5. MODELING AND ANALYSIS OF SECURITY ISSUE OF CLOUD

This section includes the security model called Security Access Control Service (SACS).

The model is analysis through the tool called Hadoop.

5.1 Security Model for Cloud Computing

After considering the issues the practical approach is needed. For this purpose the sample model is designed to implement in the cloud computing architecture. In this paper this model is reviewed and experimental results are observed. Cloud computing architecture is divided into bottom layer that includes virtualized resources and upper layer contains specific services to the user [21]. The model is shown in Fig. 4.

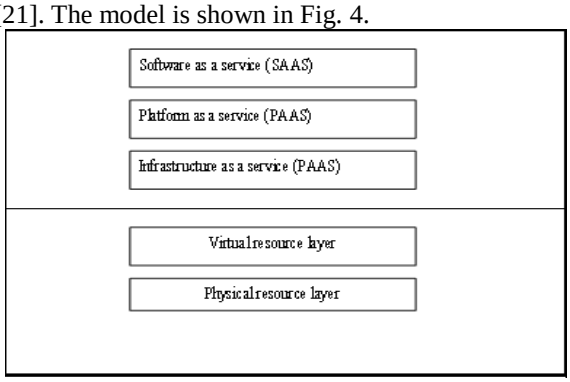

Figure 4: Cloud computing architecture

In cloud computing environment, here we introduce the idea of Security Access Control Service (SACS), which represents the composition of system modules. The block diagram is shown in Fig. 5.

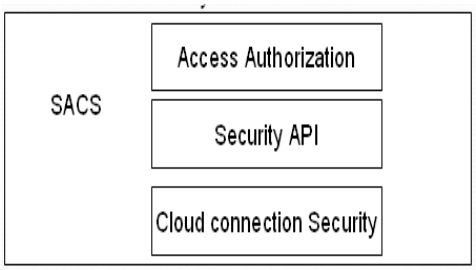

Figure 5: System module of SACS

The Security Access Control Service (SACS) will helpful toward CSP in system to implement cloud services with secure data trust. SACS includes Access Authorization, Security API, cloud connection Security modules and are described as under:

- **Access Authorization:** used to authorize to users who want to request cloud service.
- **Security API**: keeps users use specific services safely after accessing to the cloud.
- **Cloud connection security**: This ensures that the safe resource of the upper service layer provided by the bottom resource layer.

5.2 Process of SACS

The process of SACS is comprised of many steps and is described below:

1) In first step of the process the user creates a local user agent, and set up a temporary safety certificate, then user agent use this certificate for secure authentication in an effective time period It includes the name of host, user ID,

name of user , start time and end time, and different attributes for security. The user's authorization and security access is complete.

2) In second step when the user's job use the source on the cloud service layer, mutual authentication take place between user agent and explicit application, while the application ensure if the user agent's certificate is expired, a local security policy is mapped.

3) In last according to user's requirements, cloud application will make a list of service resource, and then go by it to the user agent.

5.3 Simulation Tool

The experimental results are obtained from Hadoop, an open source version of Google file system and Map-reduce programming specification. It is the software that is used to write applications that process large amount of statistics (multi-terabyte data-sets) in-parallel on big clusters (thousands of nodes) of product hardware with reliable and consistent approach. This is a distributed file base system with framework give high level API and runtime support for making and running applications on large scale data sets [22], There are many simulating tools that are available in market like CloudSim, GrimSim and cloud Analyst which are underlying projects of Melbourne university.

5.4 Experimental Results and Analysis

The proposed tool is the distributed file base system. This tool can be downloaded in Linux base operating system, Ubuntu, and the same can be run on the windows operating system. After installing this on system the individual user name Hadoop is created that is single node .Log in to this user a cluster working like cloud is designed using Java 1.6. Linux is secure operating system so attacks are generated to measure the performance. After that three common attacks are performed on the system like .mandatory access attacks, SQL injection attacks and directory traversal attacks.

- Directory traversal attack has the purpose of accessing computer files that are not proposed to be accessible. It exploits a lack of security (the software is acting exactly as it is supposed to) as opposed to exploiting a bug in the code [23].
- Mandatory access is one of the attacks used to violate the security attribute of an operating system kernel.
- SQL injection is type of attack that exploits a security vulnerability occurring in the database layer of an application and also called code injection technique.

These attacks are implemented on the machine when there is no security model is added to the architecture and results are calculated. After that through programming using Map-reduce SACS is added to the system architecture and results are recorded. Then a table is obtained and is shown in Table 4. On the behalf of the table the chart is obtained and is represent in Fig. 12 and the system performance compare is shown in Fig. 13.

5.4.1 Security Attack results

Fig. 6, Fig. 7, and Fig. 8 show the security attack result separately by identifying the attack number and attack rate using SACS and without using SACS.

5.4.2 Comparison result

The Fig. 9 shows the comparison results of all attacks (Mandatory access, directory traversal, SQL injection) using SACS model and not using SACS model.

5.4.3 System performance

Fig. 10 shows that no attacks in the first 10 minutes, the system performance which no using security model is better than the using one, the reason is the using one needs some system resources to carry out safety testing. Once the attack starts up, the performance which using security model is better than no using one. After attack, the performance is rapidly increasing. So the cloud computing with the proposed security model has the more stable performance when facing the attack threat, especially a variety of stacks at the same time.

Table 2:Data Comparison

Results	Attack number	No using SACS		Using SACS	
		Attacked number	Attacked rate	Attack number	Attacked rate
Mandatory Access	10	8	0.8	0	0
	20	17	0.85	1	0.05
	30	26	0.87	3	0.1
SQL Injection	10	9	0.9	3	0.33
	20	18	0.9	5	0.25
	30	22	0.73	4	0.13
Directory Traversal Attacks	10	5	0.5	3	0.3
	20	12	0.6	8	0.4
	30	19	0.63	15	0.5

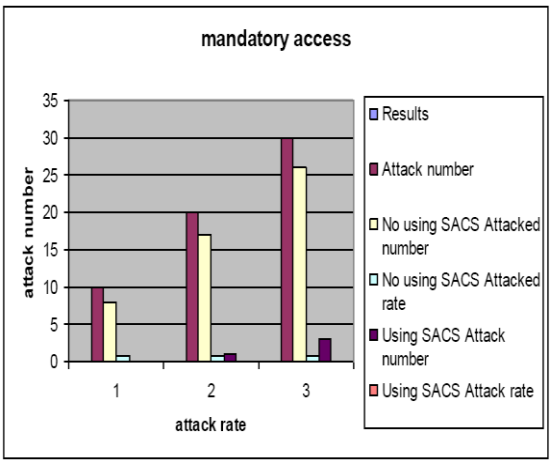

Figure 6: Mandatory access result

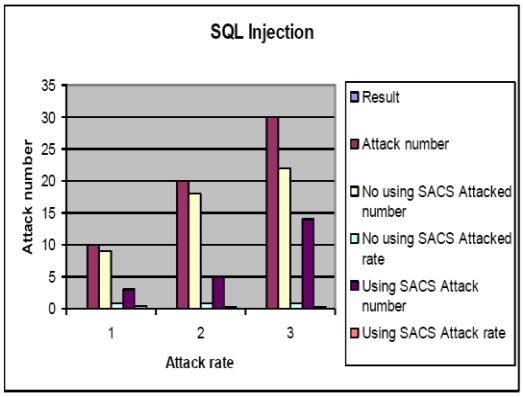

Figure 7: SQL injection

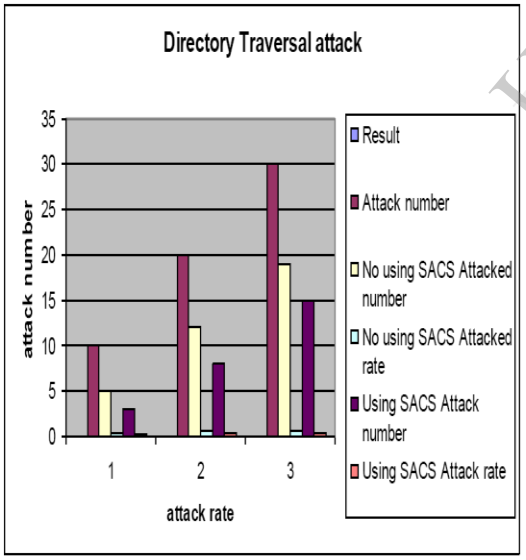

Figure 8: Directory Traversal

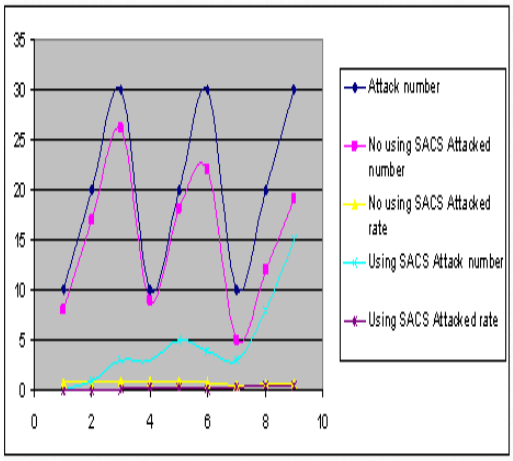

Figure 9: Comparison result using SACS and no SACS

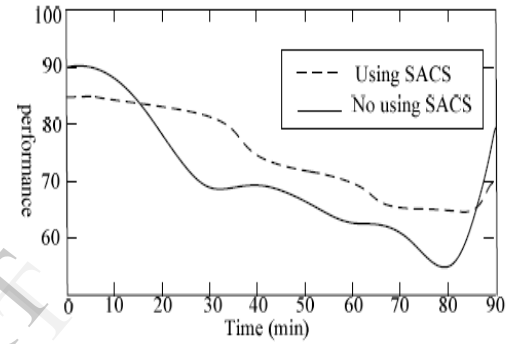

Figure 10: Performance of system

6. CONCLUSION

Cloud computing is latest development that provides easy access to high performance computing resources and storage infrastructure through web services. Cloud computing delivers the potential for efficiency, cost savings and improved performance to governments, organizations, private and individual users. It also offers a unique opportunity to developing countries to get closer to developed countries. The paper addresses the issues that can arise during the deployment of cloud services. After identify these problems some steps are explained to mitigate these challenges and solutions to solve the problems.

7. FUTURE WORK

Cloud computing is the most modern technology so lots of issues are remained to consider. It has many open issues some are technical that includes scalability, elasticity ,data handling mechanism, reliability, license software, ownership, performance, system development and management and non-technical issues like legalistic and economic aspect. Cloud computing still unknown “killer application” will establish so many challenges and solutions must develop to make this technology work in practice. So the research is not stop here much work can be done in

future. The model presented in this paper is the initial step and needs more modifications; however it can provide the basis for the deeper research on security deployment of cloud computing for the research community working in the field of Cloud Computing.

8. REFERENCES

[1] Janakiram MSV Cloud Computing Strategist; (2010), "Demystifying the Cloud An introduction to Cloud Computing", Version 1.0 – March.
[2] Adamov, A ;Erguvan, M.; (2009),"The Truth about Cloud Computing as new Paradigm in IT",IEEE International Conference on Application of Information and communication Technologies, AICT 2009.
[3] Dikaiakos, M.D; Katsaros, D.; Mehra, P.; Pallis, G.; Vakali, A.; (2010), "Cloud Computing Distributed Internet Computing for IT and Scientific Research".Vol.13 ,pp 10, Sept.-Oct. 2009.
[4] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010.ICFN ' 10.pp 23, 22-24 Jan 2010.
[5] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.
[6] R. Maggiani; (2009), "Cloud computing is changing how we communicate," 2009 IEEE International Professional Communication Conference, IPCC 2009,Waikiki, HI, United states ,pp 1, 19-22 July.
[7] Geng L; David F; Jinzy Z; Glenn D; (2009), "Cloud computing: IT as Service, "IEEE computer society IT Professional", Vol. 11, pp.10-13, March-April 2009.
[8] Basit Ali; (2009), "Ufone Launches Uconnect", published in TelecomPK.Net,12 August 2009.
[9] F. A. Alvi1, B.S Choudary ,N. Jaferry , E.Pathan "A review on cloud computing security issues &challanges "
[10] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities",5487489searchabstrSecurity& Privacy, IEEE, Vol 9, pp 50.
[11] Gansen Z; Chunming R; Jin L; Feng Z; Yong T; (2010),,"Trusted Data Sharing over Untrusted Cloud Storage Providers",2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp 97, Nov. 30 2010-Dec. 3 2010.
[12] Pearson, S.; (2009), "Taking account of privacy when designing cloud computing services",5071532searchabstract CLOUD '09. ICSE Workshop on Software Engineering Challenges of Cloud Computing, 2009. pp 44, 23-23 May 2009.
[13] Kresimir P; Zeljko H; (2010), "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.
[14] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.
[15] Popovic K; Hocenski Z; (2010), "Cloud computing security issues and challenge", 5533317searchabstractMIPRO, 2010 Proceedings of the 33rd International Convention , pp 344,24-28 May 2010.
[16] Jensen, M.; Schwenk, J.; Gruschka, N.; Iacono, L.L.; (2010), "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, 2009. CLOUD '09, pp 109, 21-25 Sept. 2009. 5708519 searchabstract
[17] Jianfeng Y; Zhibin C; (2010), "Cloud Computing Research and Security Issues", IEEE 2010 International Conference on Computational Intelligence and Software Engineering (CiSE), pp1, 10-12 Dec 2010.
[18] Jansen, W.A.; (2010), " Cloud Hooks: Security and Privacy Issues in Cloud Computing5719001 IEEE 2011 44th Hawaii

About The Authors

J.SureshBabu, received his B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru TechnologicalUniversity, Anantapur, India, in 2009. Currently pursuing M.Tech in computer science and engineering at KVSR Institute of Technology, Kurnool, India.

K.Kishore, received his MCA from Jawaharlal NehruTechnological University, Hyderabad,India. 2006; M.Tech in Computer Science from Jawaharlal Nehru Technological University, Anantapur, India.in 2012. He is an Asst.Professor atDR.K.V.S.R.I.T, Kurnool, India.

K E NareshKumar, received B.Tech degree in Computer Science and Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2006. M.Tech in Computer Science from Visweswaraya Technological University, Belgaum, India.in 2010,working as an Asst.Professor in CSE DeptatR.G.M.C.E.T, Nandyal, India.