A review on cloud computing security issues & challanges

F. A. Alvi[1, Ψ], B.S Choudary[2] ,N. Jaferry[3] , E.Pathan[4]

[1]Department of Computer Systems Engineering, QUEST Nawabshah, Sindh, Pakistan
[2]Department of Computer Systems Engineering, MUET Jamshoro, Sindh, Pakistan
[3]Department of Computer Systems Engineering, QUEST Nawabshah, Sindh, Pakistan
[4]Department of Electronic Engineering, QUEST Nawabshah, Sindh, Pakistan

Abstract

The new developments in the field of information technology offered the people enjoyment, comforts and convenience. Cloud computing is one of the latest developments in the IT industry also known as on-demand computing. It provides the full scalability, reliability, high performance and relatively low cost feasible solution as compared to dedicated infrastructures. It is the application provided in the form of service over the internet and system hardware in the data centers that gives these services. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure. When this cloud is made available for the general customer on pay per use basis, then it is called public cloud. When customer develops their own applications and run their own internal infrastructure then is called private cloud. Integration and consolidation of public and private cloud is called hybrid cloud. But having many advantages for IT organizations cloud has some issues that must be consider during its deployment. The main concern is security privacy and trust. These issues are arises during the deployment of mostly public cloud because in public cloud infrastructure customer is not aware where the data store & how over the internet.
In this paper security privacy & trust issues of cloud computing are reviewed. The paper includes some surveys conducted by IDC that show the motivation for the adoption of cloud computing. The paper identifies the issues and the solution to overcome these problems. The paper also contain the security model named security access control services SACS is analyzed through the Hadoop map reduce framework and the experimental results are obtained that compare the system performance with SACS model and without SACS model. Once the attack starts up, the performance which using security model is better than not using one. 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.

[C]orresponding Author: fizza_alvi85@yahoo.com

Keywords—Cloud Computing, SACS, Security Issues

1. INTRODUCTION

Cloud computing is latest trend in IT world. It is Internet-based computing, whereby shared resources, software and information, are provided to computers and other devices on-demand, like the electric grid. This technology has the capacity to admittance a common collection of resources on request. It is proving extremely striking to cash-strapped IT departments that are wanted to deliver better services under pressure.

Concept of this new trend started from 1960 used by telecommunication companies until 1990 offered point to point data circuits and then offered virtual private networks. But due to network traffic and make network bandwidth more efficient introduced cloud to both servers and infrastructure. The development of this Amazon played vital role by making modern data centers. In 2007 Google, IBM and many remarkable universities and companies adopted it. And in 2008 Gartner highlighted its characteristics for customer as well service providers [1].

This paper provides the guidelines and considerations required to IT enterprises for the adoption of cloud computing technology. The paper provides the awareness of cloud computing power to the IT industry by addressing the global challenges. The paper covers the issues that can arise and face in the implementation cloud computing.

- To collect information and statistics surveys conducted by the most popular and standard organisations; like International Data Corporation (IDC).

- A brief review of cloud computing security, trust & privacy issues.

- Address the security issues and challenges faced by CSP to implement cloud service, some mitigation steps and the overlook of security model that can solve some security issues in cloud environment.

The paper is further is organized as under: Section II provides the literature review. Section III includes surveys on cloud computing, Section IV contains security, trust and privacy issues and brief description of mitigation steps and solutions for these issues. Section V includes security model and experimental results and Section VI gives conclusion and future work of this research.

2. LITERATURE REVIEW

The literature identifies three different broad service models for cloud computing: a) Software as a Service (SaaS), where applications are hosted and delivered online via a web browser offering traditional desktop functionality for example Google Docs, Gmail and MySAP. b)Platform as a Service (PaaS), where the cloud provides the software platform for systems (as opposed to just software), the best current example being the Google App Engine. c) Infrastructure as a Service (IaaS), where a set of virtualized computing resources, such as storage and computing capacity, are hosted in the cloud;

Corresponding Author: fizza_alvi85@yahoo.com

customers deploy and run their own software stacks to obtain services. Current examples are Amazon Elastic Compute Cloud (EC2), Simple Storage Service (S3) and Simple DB.

The literature also differentiates cloud computing offerings by scope. In private clouds; services are provided exclusively to trusted users via a single-tenant operating environment. Essentially, an organization's data centre delivers cloud computing services to clients who may or may not be in the premises [2]. Public clouds are the opposite: services are offered to individuals and organizations who want to retain elasticity and accountability without absorbing the full costs of in-house infrastructures [2]. Public cloud users are by default treated as untrustworthy. There are also hybrid clouds combining both private and public cloud service offerings [3].

3. SURVEY CONDUCTED ON CLOUD COMPUTING BY IDC

This section includes survey conducted by international data corporation (IDC). It shows the strength of cloud computing to be implemented in IT industry and gives the potential inspiration to CSP. The section contains the survey related to the growth of cloud, security aspect, cloud is the first priority to the vendors, revenue report, future and current usage, state of cloud to the IT users and popularity survey of cloud computing.

a) Cloud growth: The Table 1 shows the cloud growth from year 2008 to 2012 [4].

b) Survey on cloud security: The Fig. 1 shows the survey on security. This represents security as first rank according to IT executives. This information is collected from 263 IT professional by asking different question related to the cloud [5], and many of the executives are worried about security perspective of cloud.

Table 1: Cloud Growth

Year	2008	2012	Growth
Cloud IT Spending	$ 16 B	$42 B	27%
Total IT spending	$383 B	$ 494 B	7%
Total-cloud spend	$367 B	$ 452 B	4%
Cloud Total spend	4%	9%	

c) Top ten technology priorities: This report displayed in Fig 2 collected at the end of 2010 by IDC. This shows that now a days the cloud computing is the first priority by organization in the field of technology [4].

d) World wide IT cloud services revenue by product/service type: The Fig. 3 and Fig. 4 show the survey collected in 2009 by IDC. This survey shows the revenue on cloud in 2009 is 17.4 billion dollars but it will enhance up to 44.2 billion in 2013 [6].

e) Current and future usage of cloud in IT: The Fig. 5 shows the graph that is collected by IDC in August 2009. It shows todays usage and future usage of Cloud in different areas.[7]

[C]orresponding Author: fizza_alvi85@yahoo.com

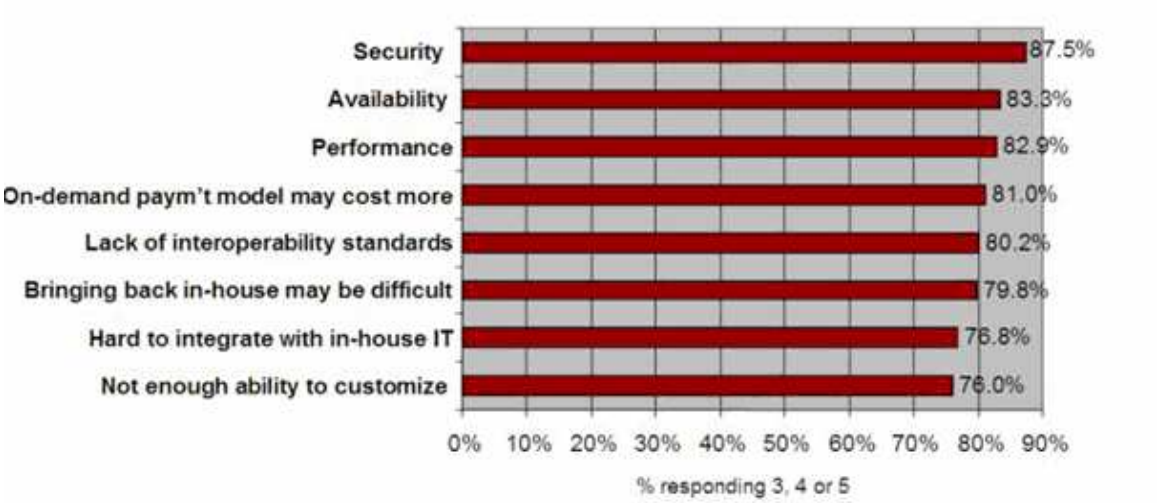

Figure 1: cloud security survey [5]

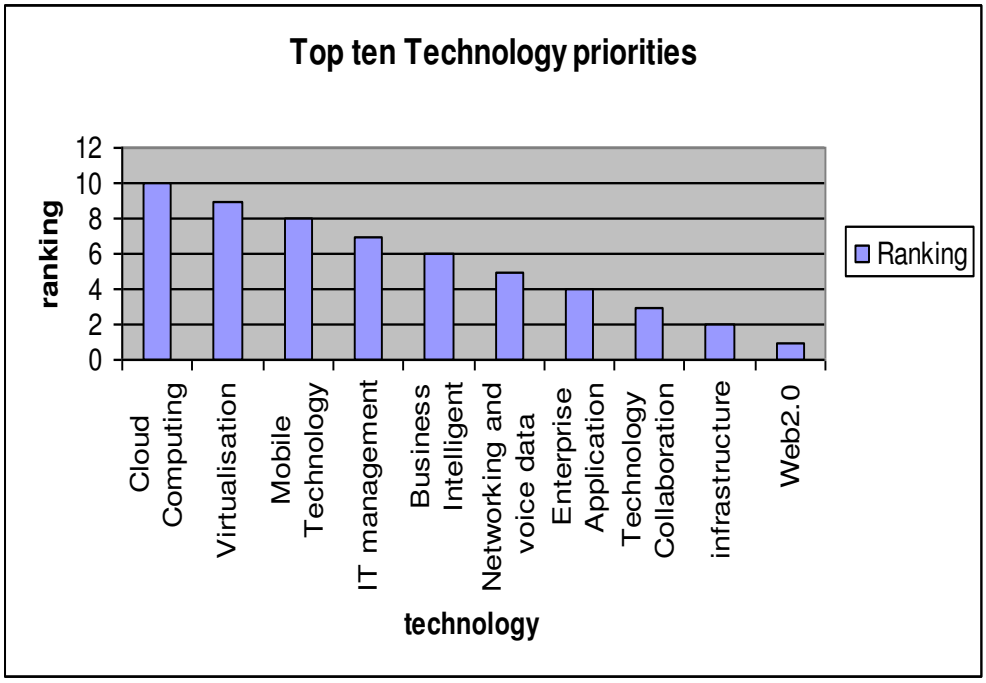

Fig. 2: Top ten technology priorities

[C]orresponding Author: fizza_alvi85@yahoo.com

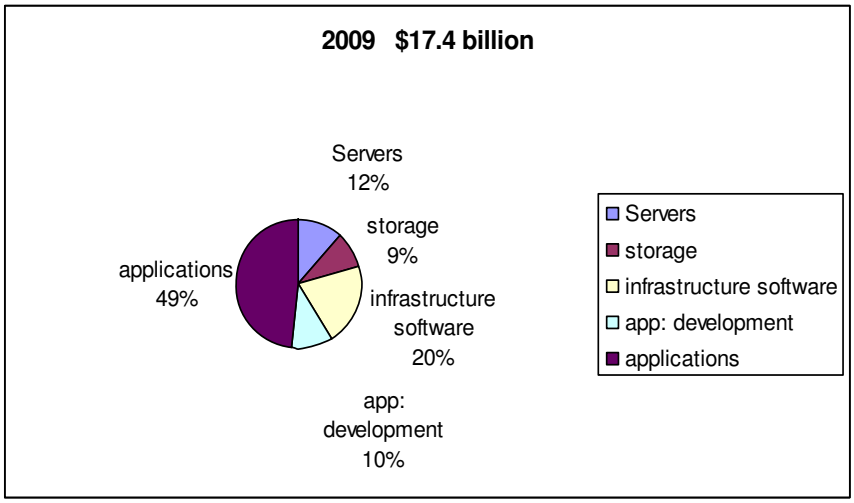

Fig. 3: 2009 revenue report

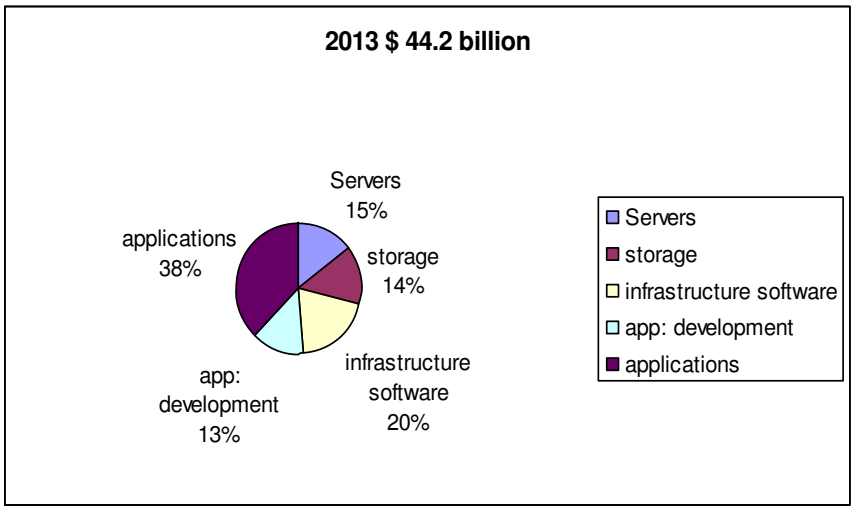

Fig. 4: 2013 expected revenue report

[C]orresponding Author: fizza_alvi85@yahoo.com

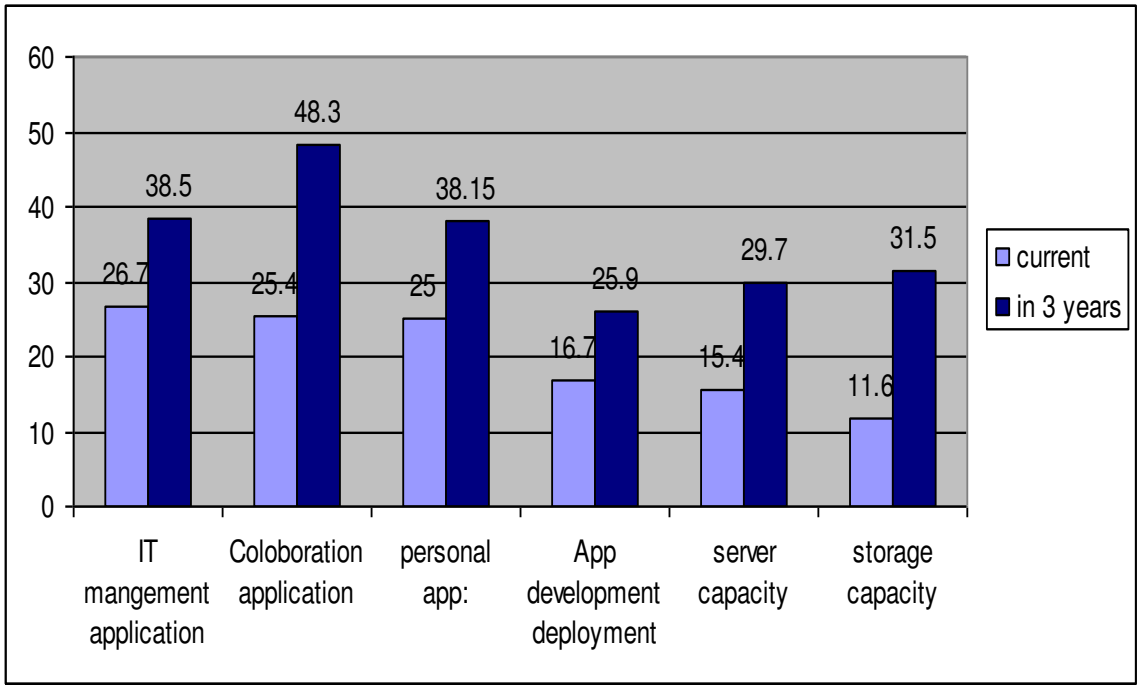

Figure 5: Current and future of cloud usage

f) Opinion for the state of cloud computing: The chart shows in Fig. 6 represents the position of cloud according to different executives. Survey conducted from 696 IT consultants about the status of the cloud, what is their opinion related to it [7]
g) Survey on popularity: This survey shows in Table 2 illustrate the popularity of cloud .It illustrates the rapid growth of cloud application, services and devices [6].

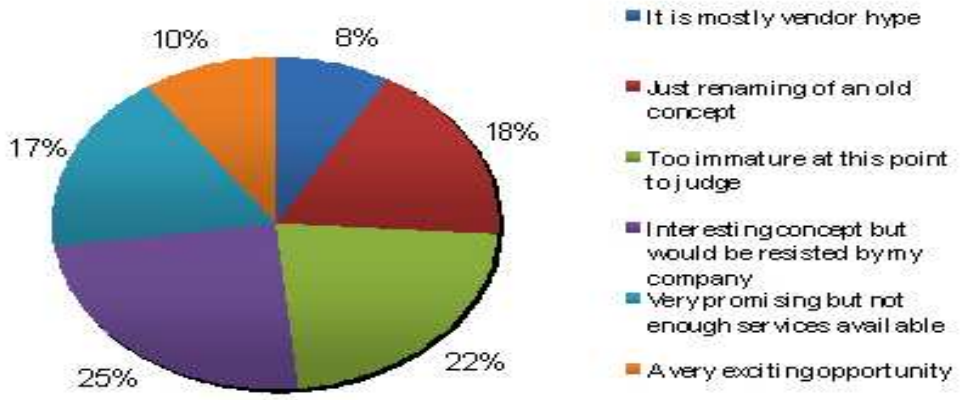

Figure 6: State of cloud computing

Corresponding Author: fizza_alvi85@yahoo.com

Table 2 : Increased Popularity

	2010	2011	%Growth
Number of Apps	2.3	6.5	82%
Number of Devices	2	4	100%
Connecting Apps to the Cloud	64%	87%	38%

4. CLOUD 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. As Pakistan 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 [10]. 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 [11] . 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 [12].

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 [13]. 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

Corresponding Author: fizza_alvi85@yahoo.com

termination, and if cloud computing provider is bankrupted or another company get data then what would happen [14]

4.1.3 Transborder 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. Due to movement of data, CP exacerbate the transborder data flow matter because it can be tremendously difficult to ascertain which specific server or storage device will be used, as the dynamic nature of this technology [15].

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 [13].

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 [16].

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 [17].

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 [16].

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 [16].

[C]orresponding Author: fizza_alvi85@yahoo.com

4.2.5 Audit

To implement internal monitoring control CSP need external audit mechanism .But still cloud fails to provide auditing of the transaction with out effecting integrity [18].

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 [19]

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 as Pakistan is now going to developed so 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 [20]. So mitigate such type of problems some action should taken place. Some steps are listed below:

- Build up an iterative policy for relocation from traditional environment to Cloud environment . Vendors in Pakistan should follow proper strategy moving from their existing system to this new evolution.
- 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 customers 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

Corresponding Author: fizza_alvi85@yahoo.com

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

Table 3 : 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

[C]orresponding Author: fizza_alvi85@yahoo.com

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. 7.

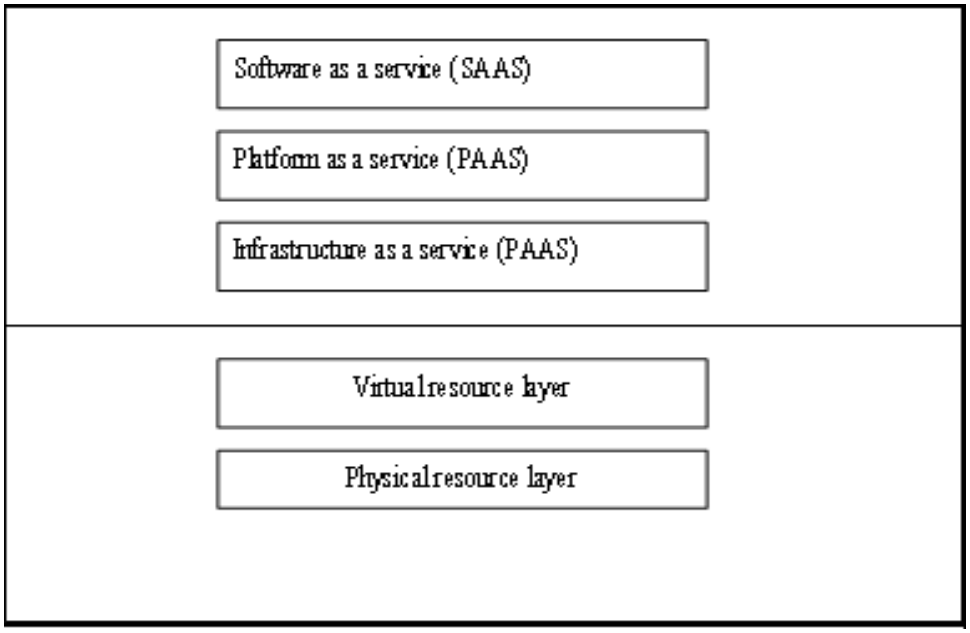

Figure 7: Cloud computing architecture [23]

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. 8.

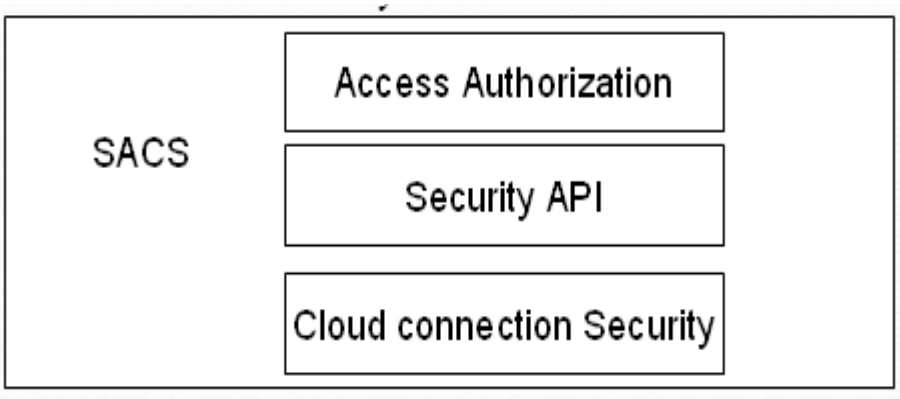

Figure 8: System module of SACS

[C]orresponding Author: fizza_alvi85@yahoo.com

The Security Access Control Service (SACS) will helpful toward CSP in Pakistan 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 are 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.

[C]orresponding Author: fizza_alvi85@yahoo.com

- 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 result 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. 9, Fig. 10, and Fig. 11 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. 12 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. 13 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.

[C]orresponding Author: fizza_alvi85@yahoo.com

Table 4: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

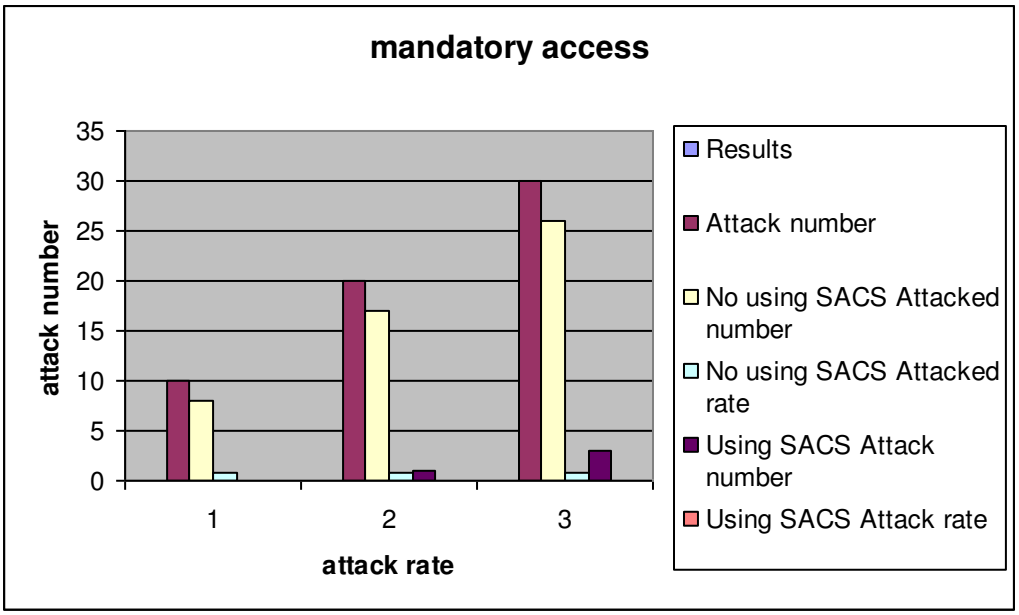

Figure 9: **Mandatory access result**

Corresponding Author: fizza_alvi85@yahoo.com

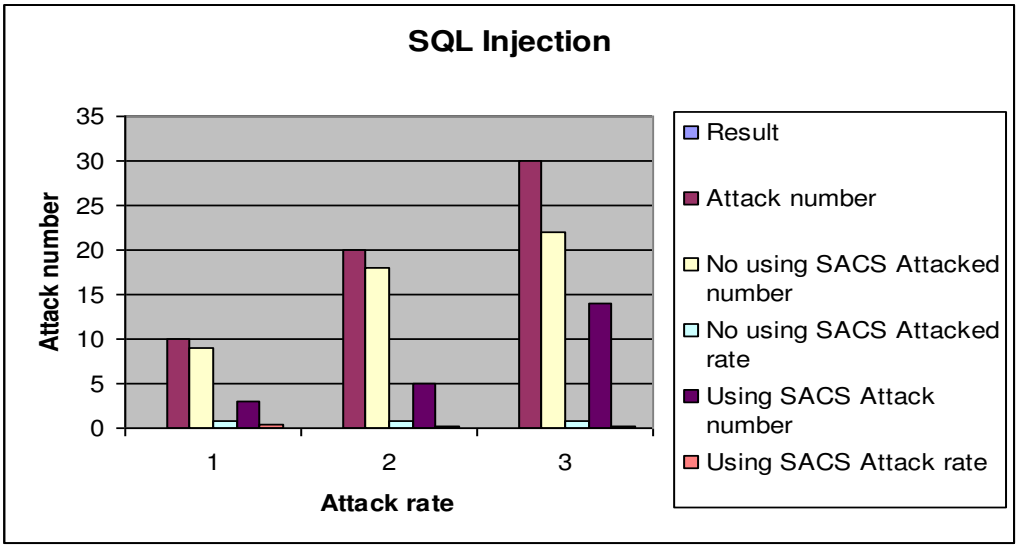

Figure 10: SQL injection

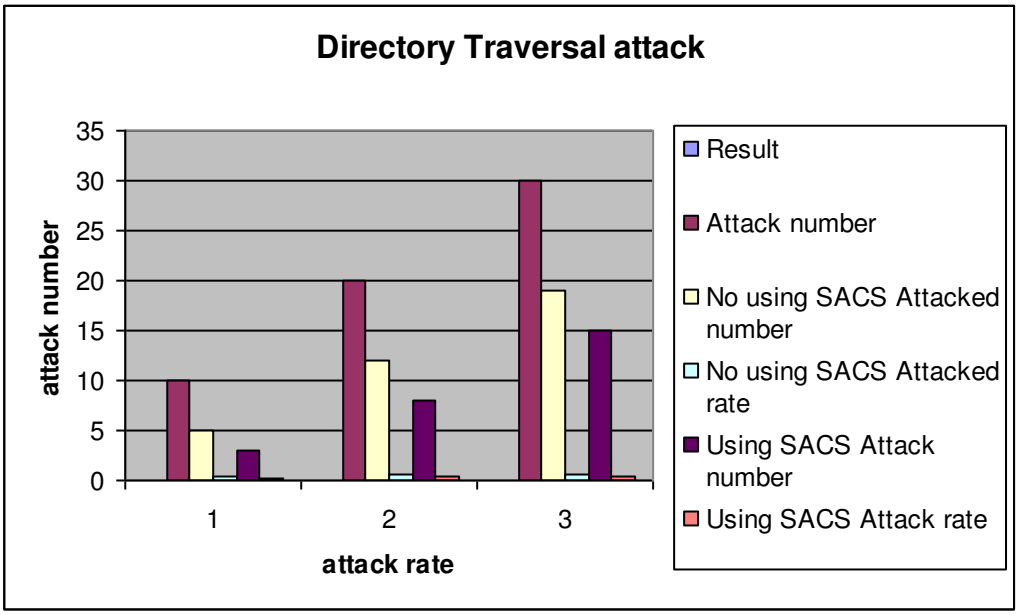

Figure 11: Directory Traversal

[C]orresponding Author: fizza_alvi85@yahoo.com

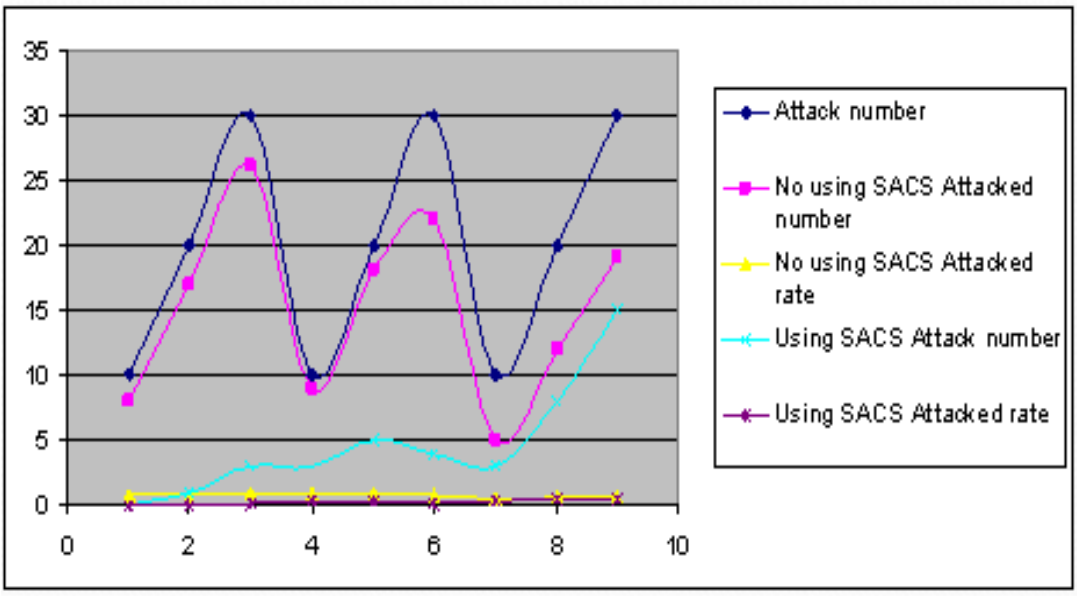

Figure 12: Comparison result using SACS and no SACS

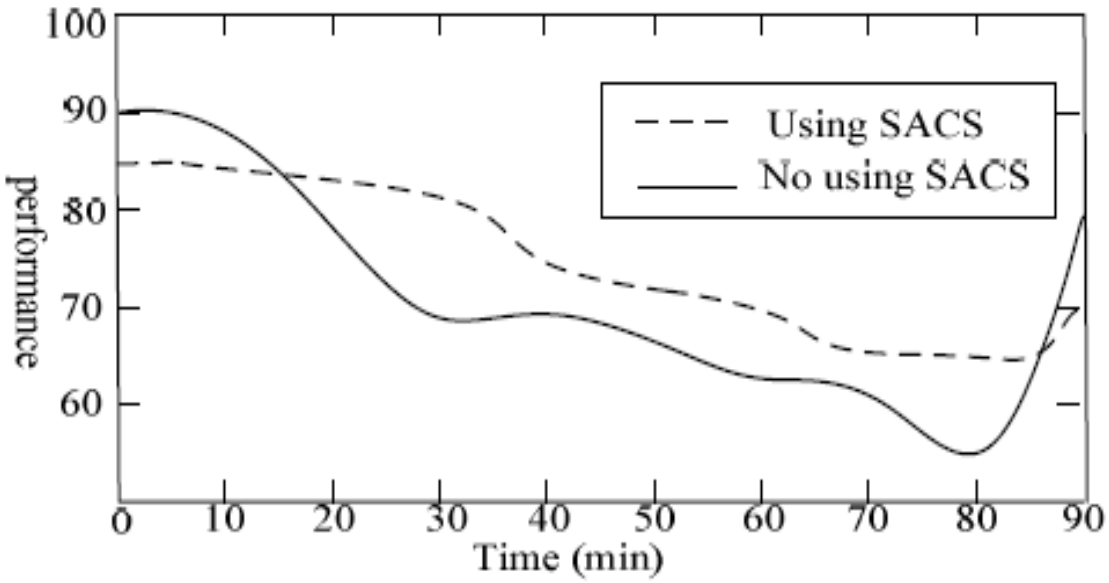

Figure 13: Performance of system

Corresponding Author: fizza_alvi85@yahoo.com

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. Developing countries like Pakistan can take the benefits of cloud computing by implementing it in its e-government projects. 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.

Acknowledgment

Authors are very grateful to Mehran University of Engineering and Technology, Jamshoro, Sindh, Paksitan and Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Sindh, Pakistan for providing resources and environment to carry out this research.

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.

Corresponding Author: fizza_alvi85@yahoo.com

[9] Muzzammil Sheikh; (2011), "PTCL Launched EVO USB become Wi-Fi Hotspot", The Frontier Star (Northwest Frontier Province, Jan 26 2011 Issue.

[10] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities",5487489 searchabstrSecurity & 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",5071532 searchabstract 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 International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2011.

[19] Tian L.Q; NI Y,LING; (2010) , "Evolution of user Behavior Trust in Cloud Computing", 2010 International Conference on Computer Application and System Modeling (ICCASM 2010),Vol. 7,pp V7-567, 22-24 Oct. 2010.

[20] Mathur, P; Nishchal, N.; (2010), "Cloud Computing: New challenge to the entire computer industry", 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010), pp 223.

[21] Yuefa D; Wu B; Yaqiang G; Zhang Q; Tang C; (2009), " Data Security Model for Cloud Computing", Proceedings of the 2009 International Workshop on Information security and Applications (IWISA 2009)

[22] Dean and S. Ghemawat; (2010), "MapRduce: Simplified data processing large clusters", communication of the ACM, Vol.51, pages 107-113.

[23] Xue J; Zhang J.J; (2010),"A Brief Survey on the Security Model of Cloud Computing",2010 Ninth International Symposium on Distributed Computing and Applications to Business, Engineering and Science.

Corresponding Author: fizza_alvi85@yahoo.com