# A New Approach for Providing Security Mechanism in Cloud with Possible Solutions and Results

Sarvesh Kumar[1] Punnet Kumar[1] Suraj Pal Singh[2] Ajit Saxena[3]
Computer Science and Engineering[1-3]
Lovely Professional University[1], Punjab [3]Eshan College of Engineering[2], Mathura
Sri Satya Science Institute of Science and Technology[3], MP

## ABSTRACT

In the field of IT technology, cloud computing is a next big thing in IT market. It is just internet based computing and on demand computing which gives reliability, scalability, availability compared to dedicated infrastructure. The main issues in cloud computing is security, trust and privacy issues. These issues arise at the time of deployment of cloud computing services in public and private cloud. In this paper security and privacy issues are reviewed and gives a proposed mechanism for securing data in cloud and also used Microsoft window azure tools for SACM (security access control mechanism) , and compare the system with SACM tools and NO SACM tools. The implementation result will show that security model is better than using SACM tools. It also defines web hosting in old manner and web hosting in cloud manner. In the future scope we can see multi tenancy security issues in cloud computing.

## Keywords

cloud computing, IaaS, PaaS, SaaS

## 1. INTRODUCTION

The idea of cloud computing has evolved with increased popularity of applications like face book, Gmail and you tube. When you use these applications, our data is not stored in our computer; instead the application is provided to you over the internet and the data is generated via that applications is stored in the provider's data centre which is stored in the cloud. Data is only copied to our computer's cache memory to allow to user to access it and view it. The most widely used definition of the cloud computing model is introduced by NIST as "a model for enabling convenient, on demand network access to shared pool of configurable resources ( e.g. Networks, servers, storage, application and services ) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

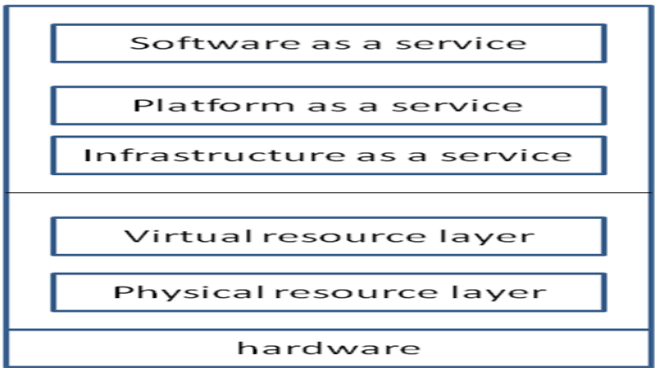


**Fig 1.1 It is a general architecture of cloud also called cloud stack. In cloud stack, each layer represents service model.**

In IaaS, where resources are managed physically or virtually. In PaaS, in which services are provided as an environment for programming (windows azure), and at the top layer SaaS offers, software applications as a service. This paper is further organized as under: section [2] provides literature review, section [3] provides security trust and issues in cloud computing, section [4] proposed approach of security architecture, section [5] summarizes the conclusion work and section [6] defines the future work.

## 2. Literature Review:

Grushka et al [2] described the security based on three participants of cloud system that is service use, instance and cloud provider. Balchandra et al [3] discussed on SLA specification, data location, data security and data management and data recovery in cloud computing. Subashhiki et al [4] have discussed the security issues based on three service models( IaaS, PaaS, SaaS). Sarveshkumar et al [5] described threats and issues in cloud computing and describes attacks in different different levels in private clouds. Zhifeng et al[6] discussed on cloud computing vulnerabilities and five main security issues on authentication ,confidentiality, privacy, integrity and availability.

Thus literature defines three define services models in cloud computing:

a. SAAS: where applications are hosted and delivered online with the help of web browser. E.g. Google Docs, Gmail

b. PAAS: cloud provides the platform to use that application. E.g. Google App. Engine, Microsoft windows Azure.

c. IAAS: a set of virtualized computing resources such as storage and computing capacity in the cloud. E.g. Amazon.

## 3. Security, Trust and issues in cloud computing:

Cloud computing is new emerging technology for the business perspective of view and IT perspective of view. It is shared resources, lower cost and priced on demand. Due to many characteristics it impacts on security, issues in cloud computing.

### 3.1 Privacy issue:

Every people want security of his private and sensitive information thus the outsourcing of data is major privacy

issues in cloud computing environments, out sourcing of data means customers loss their physical control over data.

a. **Loss of physical control over data:** In the SaaS environment like Gmail account, when the user login Gmail account, the users loss their physical control where the data is stored and what type of operations are performed on those data. Thus in this issues user's information is processed in the cloud, so there is the risk of manipulation of data. In Gmail account, users have no admin control; admin control is managed by cloud service provider.

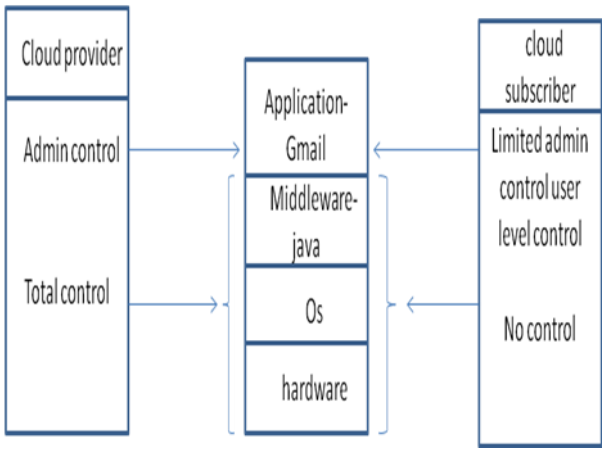


**Fig 3.1.a privacy issue in cloud computing**

b. **Issue of multi Tenancy:** cloud are used to IT resources efficiently and security. Multi-tenancy, it is just like building apartment, where many tenant share common infrastructure for building but have walls and doors give them privacy from other tenants, thus there are issue of share IT resources among multiple applications and tenants.

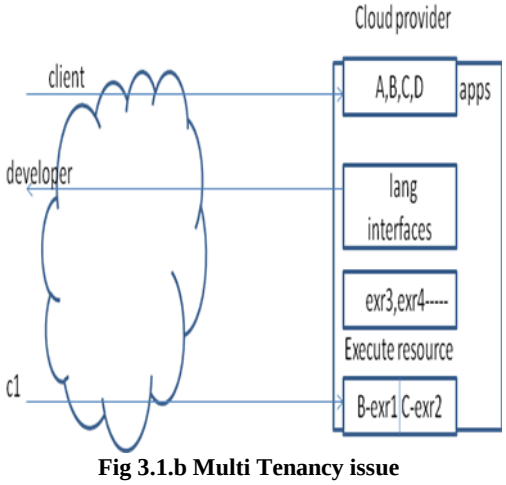


**Fig 3.1.b Multi Tenancy issue**

c. **Issue of pricing model for customers:** cloud computing is based on on-demand pricing model based on server utilization, cpu utilization ,band width and storage utilization , thus main issues is that attacker manipulates the pricing model and causes the unmanageable costs for customers.

**3.2 Security issue:** security issues includes problem of authentication, authorization, integrity and confidentiality of data.

**3.3 Trust:** trust includes assurances and confidence that the processes will function in an expected ways [7]. Trust may be human to machine (digital signature), machine to human (verification), human to human and machine to machine (hand shake protocol).

## Issues arise in technologies:

| area / Tech. | security | privacy | trust |
|---|---|---|---|
| virtualization | integrity | Segaration of personel data | Hypervision permits loss of control |
| Grid technology | Availability | | interoperability |
| Web services | Intergrity and confidentiality | Security and confidentiality | interoperability |
| SOA | integrity | | Security credentials |

## 4. Problem of securing data in cloud:

The problem with data that is stored in the cloud is that it can be located anywhere in the cloud providers system in another data centre or in another country. For client/server architecture, firewalls works as a security parameter but in the cloud ecosystem. There is no physical system to protect the data. thus to protect of cloud storage assets ,we want to find way to isolate data from clouds.

## 4.1 Possible solutions:

An approach to isolate software in the cloud from direct client to create layer to access the data.

Two services:

1. Broker with full access to storage but no access to the client.
2. Proxy with no access to storage but access to both client and broker.

The location of broker and proxy is not important, they can be local or in the cloud, what is important is that two services i.e. The direct path between the client and data in the cloud.

**Steps:** when a client makes a request for data...

1. The request goes to external service interface of the proxy which is practically trusted.
2. The proxy using its internal interface, forward to the broker.
3. The broker requests the data from cloud storage system.
4. Storage system returns the result to the broker.

5. Broker returns the result to the proxy.
6. Proxy completes the response by sending the data requested to the client

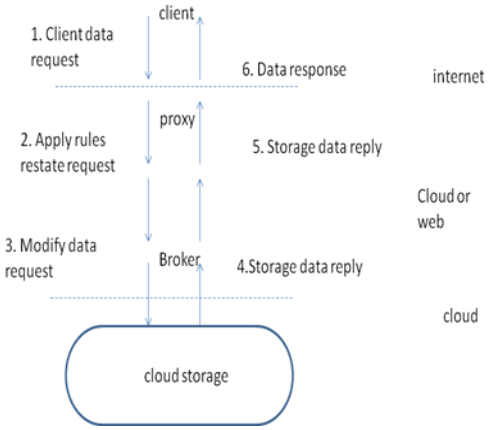


**Fig 4.1 In this design, direct access to cloud storage is eliminated in favour of a proxy/broker service.**

## 4.2 2nd possible solutions:

If we use multiple encryption keys can separate the proxy service from the storage, account. Using two separate keys to create two different zones.

a. Untrusted communication between the proxy and brokers services.
b. Trusted zone between broker and cloud storage.

Because of data stored in the cloud is usually stored from multiple tenants each other has its own unique method for separating one customer's data from one another. Most cloud services provide store data in encrypted form. Goal of encrypted cloud storage is to create a virtual private storage system that maintains confidentiality, authentication, authorization and integrity. Microsoft allows up to fine security accounts per client and you can use these different accounts to create different zones. On Amazon web services, you can create multiple keys and rotate these keys during different reasons. Although encryption protects data from unauthorized access, it does nothing to prevent data loss, indeed for losing data encrypted data is to lose the keys that provides access to the data. Thus we need a key management. Keys should have different life cycle.

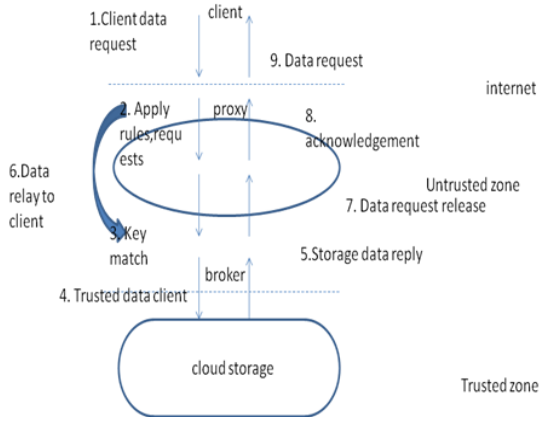


**Fig 4.2 The creation of storage zones with associated encryption keys can further protect cloud storage from unauthorized access.**

## 4.3 Proposed solutions for these issues:

A solution approach for cloud customer and cloud service provider that offers services within cloud security environment.

**Tabel 4.3 solution description of issues**

| Solution | Description |
|---|---|
| Policy design | • Information principle are applicable<br>• For term and conditions |
| Standard mechanism | • Confidential data<br>• Geographically distributed data |
| Availability | Cloud service provider should follow data tracking and data handling |
| Mechanism for security, privacy and trust | • Intelligence software<br>• Information should go through cloud service provider and CSP should be fully trusted. |
| Integrity | • Encryption of data between putting data in the cloud<br>• Decryption of data before accessing data in the cloud |

## 4.4 Proposed Result:

| Result | Attack no. | No using SACM | | Using SACM | |
|---|---|---|---|---|---|
| | | Attacked no. | Attacked rate | Attacked no. | Attacked rate |
| Data Tampering | 10 | 9 | 0.9 | 2 | 0.2 |
| | 20 | 14 | 0.7 | 5 | 0.25 |
| Disclosure of confidential data | 10 | 7 | 0.7 | 3 | 0.3 |
| | 20 | 7 | 0.35 | 4 | 0.2 |
| Side channel attacks VM to VM | 10 | 5 | 0.5 | 4 | 0.4 |
| | 20 | 8 | 0.4 | 7 | 0.35 |

This result is obtained from window azure tools of Microsoft account. We used Asp.net on Microsoft windows 7 os and creating Microsoft account for windows azure and websites hosted and perform these security issues data tampering, disclosure of confidential data and side channel attacks with security access control mechanism and compare the result with SACM mechanism and NO SACM.

## 5. Conclusion

Thus cloud computing is latest technology for achieving high performance computing through web services. It gives cost saving, improve performance, efficiency to organizations, private and individual users. In India , cloud computing can be beneficial for adapting these kind of services. This paper discuss on privacy, security architecture of cloud computing and a new model for providing security in cloud computing and also gives a proposed solution to these issues. This paper also gives the result with services access control mechanism for attacks likes disclosure of confidential data, data tempering and side channel attacks.

## 6. Future work

Cloud computing is another technology and a lot of issues involves related to security. Some of the open issues related to multi-tenant issues architecture, license software, own ship, perform and system development. Peoples can research on multi tenant security architecture with SaaS, PaaS, and IaaS. Customers can share the same code base and data is stored on same set of tables with tenant ID. The future work describes in terms of multi tenant issues in cloud computing.

## 7. References

[1] An Analysis of the cloud computing security problem.

[2] N. Grushka. M.Tenson ," Attack Surfaces: A Taxonomy for attacks on cloud services," cloud computing, IEEE international conference on,pp-276-279,2010 3rd international conference on cloud computing,2010.

[3] Balchandra Reddy Kandukuri, Ramakrishna paturi and Atann Rakshit "cloud security issues" in proceedings of the 2009 IEEE international conference on services computing, 2009,pp 517-520. Forman, G. 2003. An extensive empirical study of feature selection metrics for text classification. J. Mach. Learn. Res. 3 (Mar. 2003), 1289-1305.

[4] S.Subhashint and V.Kavitna" A survey on security issues in services delivery models of cloud computing," J. Network and Computer applications,vol.34 jan 2011,pp1-11.

[5] Sarvesh kumar, Nilesh Kumar dubey," cloud computing ( A survey on cloud computing security issues and attacks in private clouds)," International journal of Emerging trends in Engg. And Development " issue 3,vol.1,jan 2013.

[6] Zhifang Xiao and Yang Xiao," Security and Privacy in cloud computing", IEEE communication surveys & Tutorial, march 2012.

[7] RAND Europe / time lex /University of Warwick.

[8] Z. Xiao, N. Kathiresshan, and Y. Xiao," PeerReview Re-evalution for Accountability in Distributed systems or networks," International J. Security and Networks(IJSN),2010,vol.7 No.1 in press.

[9] Z. Xiao, N.Kathiresshan, and y. Xiao," A survey of Accountability in computer networks and distributed systems," (wiley journal of) Security and communication networks ,accepted.

[10] E.Keller, J.Szefer, J.Rexford and R.B. Lee," Nohype:virtualized cloud infrastructure without the virtualization," in proc. 37annual international symposium on computer architecture, New York, NY, USA, 2010,pp 350-361.

[11] Q.Chai and G. Gong,"On the(in) security of two joint encryption and error Correction schemes," International j. Security and networks,vol.6 No. 4,2011 pp. 181-190.

[12] Z. Wang and R.B.Lee," A novel cache design architecture with enhanced performance and security," IN 41st IEEE/ACM international symposium on microarchitecture, pages 494-505, june 2007.

[13] R. Maggiani;(2009)," cloud computing is changing how we communicate," 2009 IEEE international Professional communication conference, IPCC 2009,Waikiki, HI, United states, PP1,19-22 july.

[14] Geng L,David F,Jinzy Z; Glenn (2009) ," cloud computing IT as a service," IEEE computer society IT professional ", Vol.11,pp 10-13, March-April 2009

[15] cloud security alliance(CSA)." Top Threats of cloud Computing V 1.0," released March 2010.

[16] K.D. Bowers, A. Juels and A.Opera,"HAIL: a high Availability and integrity layer for cloud storage," Proc. 16th ACM conference on computer and communication security, 2009, pp. 213-222.

## Websites:

[1] http:// www. Technopulse.com

[2] http:// www.oasis-open.org/comittees/kmip

[3] IEEE 1619.3 (https://sisuog.net/index. php?option= com_docman).