Architectural Data Security in Cloud Computing

Dr.P.K.Rai [#1], Rajesh Kumar Bunkar [*2]
[1]*Computer Canter APS University Rewa, India*
[2]*Research Scholar MGCGV Chitrakoot, Satna, India*

***Abstract*—** Cloud Computing sees a methodological and educational shift of computing assessment provision from being provided locally to being provided remotely, and by third-party examine provider. Data that was once housed under the security area of the service user has now been placed under the protection of the service provider. Users have misplaced control over the safety of their data: No longer is our data kept under our own watchful eyes. This paper shows data canter model for cloud computing and architecture of cloud computing.

***Keywords*—** Cloud Architecture, Data Security, Data centre Security issues.

I. INTRODUCTION

Cloud Computing is the name given to the recent drift in computing overhaul provision. This development has seen the technological and cultural shift of computing service provision from being provided locally to being provided remotely by third-party service providers [1].The use of encryption schemes is often describe through an analogy depict the transmission on a plain-text message M from one entity, A to another entity, B. Here A wishes to ensure that only B will be clever to read M. This analogy has persist to its ability to describe a prevalent communication style, that of uncast communication. The consumer has effectively lost control over how their data is human being stored, common and used, and also over the security used to protect their data. Moreover, it can be the case that a secret employee of the service provider will have access to your data for legitimate purposes but will abuse this power for their own means [9].

Definition of Cloud Computing

Cloud Computing is the cause célèbre among tech analyst and has led to the term 'Cloud Computing' as an umbrella term being applied to differing situations and their solutions.

The term 'cloud' has been used conventionally as a figure of speech for networks and helps abstract over inbuilt problem.**"** large pool of clearly utilizable and accessible virtualized resources (hardware, growth platform and/or services).These assets can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of assets is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs**."**

A cloud can be one of the following types:

Public: Constituting in public accessible services that are accessed over the Internet and are often described using the term "The Cloud".

Private: These are private services deployed on private networks. Such clouds may also be managed by third parties.

Hybrid: The arrangement of services presented both privately and publicly. For example core-services may be offered on a private cloud; other services originate from public clouds. Definition is based on five attributes that can be used to describe a cloud-based scheme. They are:

Multi-tenancy: The sharing of assets being offered by the service providers to the clients at the network, host and application level.

Massive Scalability: The capability to scale the storage space, bandwidth and systems offered to pro-portions inaccessible if performed by the organization itself.

Elasticity: clients can hurriedly and dynamically increase and decrease the assets required as needed.

Pay-as-you-go: Clients only pay for the assets they consume such as processing cycles and disk space.

Self-Provisioning of Resources: Customers have the ability for the self-provisioning of resources.

Benefits of Cloud Computing

Many of the benefits to be had when using Cloud Computing are the less significant operating cost connected. At the infrastructure level, effective images can be scale and tapered with complete disregard for any associated hardware costs such as equipment procurement, storage space, safeguarding and use. This is all taken care of by the service provider and will be factored into the payment for the service: capital expenditure has been converted into operational expenditure. Resources within the cloud can be treated as a service, an 'unrestricted' medium. At both the platform and software level similar profit are see. Aspect such as software mechanism, operation and safeguarding are virtually missing. This is in use concern of by the contributor inside their individual infrastructure. The check user only pays methodological support. Service providers at the

SaaS level, often advertise features that allow users to work in partnership and cooperate with each other, in concurrent, within the scope of the service being accessible. For example, Google Docs allows users to edit documents at the same time and for users to see each other's edits in concu rrent.

II-Data Canter Model for Cloud Computing

we discuss the material constructions of Clouds the Data Canter form is a accepted option. This form stipulate clusters of machines running high-quality, dedicated hardware and software to give the infrastructure for the large scale provision of virtualized assets [5] [3].Though a consumer can access the virtualized resources directly, when managing their resources, consumers interact with a Cloud Controller that mediates the interaction between the consumer- The physical machines; and virtualized resources owned by the consumer. Figure 1 illustrates a rather simplified view of this data canter model.A more interesting realization of clouds is the Adhoc model in which the existing (idle) computing power within an enterprise is tapped to provide the required infrastructure.

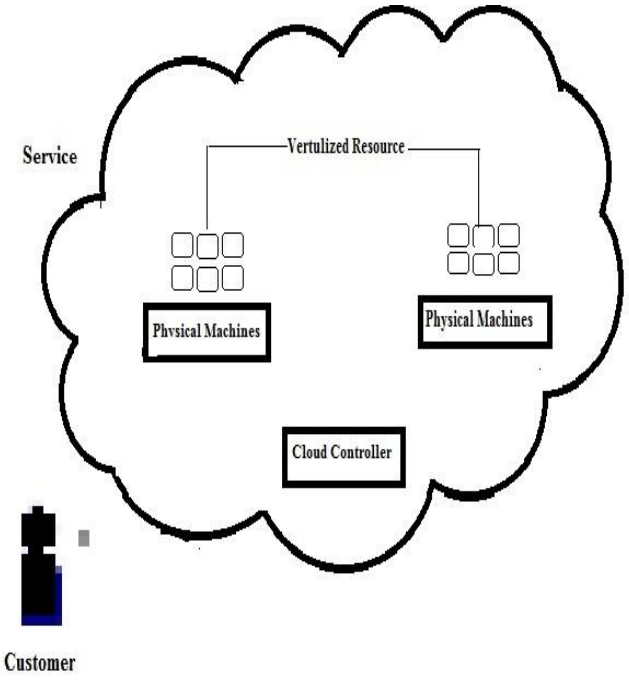

Figure 1: Data Canter Model for Cloud Computing

III.Cloud Computing Security Issues

Security issues approach under many guises both technological and socio-technical in starting point. To cover all the security issues possible in the cloud, and deeply, would be extra special a job not suited even for Heracles himself. Existing efforts look to provide taxonomy over the issues seen. The Cloud Security Alliance[1] is a non-profit organization that seeks to promote the best practices for providing security assurance within the cloud computing landscape. In Hubbard, Sutton et al. [4] The Cloud Security Alliance categorizes seven threats. These ares -

1. Abuse and Nefarious Use of Cloud
2. Insecure Application Programming Interfaces
3. Malicious Insiders
4. Shared Technology Vulnerabilities
5. Data Loss/Leakage
6. Account, Service and Traffic Hijacking
7. Unknown Risk Profile

Abuse and Nefarious Use of Cloud: Genuine CSPs can be injured for nefarious purposes, supporting criminal or other untoward activities towards consumers. For example, services can be used to host malicious code or used to facilitate communication between remote entities i.e. bonnets. The emphasis is that legitimate services are used with hateful intention in mentality. Other issue see contain the stipulation of purposefully insecure services used for data capture.

Insecure Interfaces and Application Programming Interfaces: Data placed in the Cloud will be accessed through Application Programming Interfaces (APIs) and other interfaces. Malfunctions and errors in the boundary software, and also the software used to run the Cloud, can direct to the unnecessary disclosure of users data and hold responsible ahead the data's integrity. For example a (fixed) defect in Apache, a popular HTTP server, permissible an attacker to gain complete control over the web server [2].

Malicious Insiders: Although a CSP can be seen as being honest their employees may not be. A malicious insider is an employee of the CSP who abuses their position for information gain or for other nefarious purposes e.g. disgruntled employee. Regardless, of the employee's motivation the worrying aspect is that a surreptitious employee will have access to consumer's data for legitimate purposes but will abuse this power for their own means [9].

Shared Technology Issues: A more interesting form of confidentiality issue relates to the construction of a cloud and the services themselves.

Virtualization Issues: The underlying virtualization architecture allows IaaS service providers the ability to host several machine images on a single server. Ristenpart, Tremor et al. [11] discuss practical attacks on services, concentrating on Amazon EC2.

Service Aggregation: Aggregated services offer services based upon the functionality offered by existing services. Often aggregated services offer the combined functionality of existing services allowing for rapid tune-up structure. But, tune-up aggregation present customers with a number of attractive harms

[10].Data are now being shared across multiple service providers whose privacy policies will also matter to modify. Beneath whose confidentiality strategy is the data govern by, how to combine the two policy? additionally, examine aggregation can happen in an ad-hoc and rapid manner implying that less stringent controls could have been applied to the protection of data, increasing the likelihood of a problem.

Data Loss or Leakage: I nsecure APIs can lead to data loss or the unwanted exposure of information, consumers can also lose their information through other means.

Availability Issues: Availability issues are when user's data is made inaccessible to the consumer. The data has been made unavailable. Such a lack of accessibility can be a result of access privilege revocation, data deletion or restricting physical access to the data itself. Ease of use issues can be recognized to an attacker using flooding based attacks [6]. For example, Denial of Services attacks, attempt to flood the service with requests in an attempt to overwhelm the service and cease all of the services intended operations.

Data Leakage: Data leakage stems is the disclosure of information that, though hidden, is deduced from freely available information.

Account or Service Hijacking: When communicating with the CSP malicious entities may seek to affect the integrity and authenticity of the user's communication with the CSP and vice versa. There are several ways in which the integrity and authenticity of a user's session can be impugned [7].

Unknown Risk Profile: Risk Management is a business process that users can use to identify and mitigate threats. It allows users to decide their present position towards the security of their data. Auditing information such as software version, code updates, current security practices, intrusion attempts et cetera, are used as a basis for formative this position.

IV. Data Security Requirements

Security requirements will aide when developing or analysing any solution, and also when describing the security offered. It is highlighted that when describing the possible threats to data in the cloud two viewpoints must be taken into account: T he users and, The CSP.This arose as data is either in the cloud or not in the cloud. Thus the security requirements will be the responsibility of: the user; the CSP; or of both the user and the CSP.This shall be addressed for each security requirement presented.

Confidentiality: The data that is to be entrust to the cloud may be of a perceptive nature and will thus be subject to several privacy dealings. Although privacy of data is first and foremost seen as being solved via encryption, as discussed in Broad foot and Martin[8].User and Resource Privacy: Within the Cloud, confidentiality of data also extends to how the data is being processed/used and also the users actions. The means by which CSP can store or process the data is bound by law and these laws must be adhered to. Such data include and is not incomplete to: audit records representing admittance attempt and changes (and their results) to the data; property of the data including volume, access policies and source; and even the reality of the data itself.

Deducible Data:The hidden information pertaining to an individual can be deduced from existing information. An attacker should not be able to use existing information or information relating to the confidential data i.e. meta-data to deduce any other information. Such attacks should be made as difficult as possible. For those who have multiple personae on the web relating to the different facets of their private life. The ability of an attacker to link the two should be hard.

Remote Access: The Cloud, by nature, is inherently a 'public place'. Services are exposed over HTTP, a public medium. Admittance to these services needs to be controlled and admittance kept to certified personnel. Moreover as the data is held remotely, trust needs to be established with the service and with the security provided by the service over the data itself. Access to the data needs to be regulated. CSPs must ensure that entities trying to access the data are not only who they say they are (authentication) but also that they have the right to do so (authorization) This is made more difficult as CSP will be interacting with multiple users from multiple companies (domains) each of whom will require different management and access policies; and all done remotely. Authentication CSPs must ensure that those trying to access the service are who they say they are. Unauthenticated users and impostors should not be able to access the data. The identity of the entities must be assured. This will imply some form of identity management.

Non-Repudiation: Both the CSP and user should not be able to deny the origin or refute the integrity of data. Moreover, a verifiable record of the data's lifecycle should exist. The lifecycle of the data and the operations performed on the data should be attestable if a CSP attempts to defraud a user and vice versa. This is especially important if flexible payment models are used. Integrity and Consistency. The mobility of data within the cloud only increases the threats that can affect the integrity of data. Data is being transported to-and-from the user and service providers, and also internally within the cloud. The integrity of the data must be guaranteed when it has been placed within the Cloud. Consistency problems can arise from omission and

commission failures. Omission failures occur when an entity fails to act upon input. Commission failures are those that occur when an entity though responds to input the output is not what was expected. It is possible for hardware to fail or connections to be lost at which time the data may be in an inconsistent state or unrecoverable. If data is replicated for some reason e.g. to combat availability, scalability or archival purposes, the consistency of the replicated data must be ensured.

Availability and Fault Tolerance: Another problem with entrusting data to a service provider is ensuring the availability of the data once it has been placed within the cloud i.e. resource availability. This is essentially a guarantee that can only be made by the CSP them. Users only have the assurances made by their service provider that data will be made available. If the data were to be made unavailable for some reason, users will not be able to access their data and become inconvenienced. The inconvenience caused could also lead to profit loss for both the user and the CSP. Moreover, internally the nodes within the Cloud must also be resilient to node failure and the data held on the nodes must still be available. Internally the Cloud must be fault tolerant.

V. Architecture of cloud computing [12]

The architecture of cloud computing is residential at three layers: application, infrastructure, and platform. These three layers are implemented with virtualization and correspondence of hardware and software assets provisioned in the cloud. The services to public, private, hybrid and Community clouds are expressed to users through network sustain over the internet involved. It is clear that the infrastructure layer is developed first to support IAAS services. This infrastructure layer serves as the base for building the platform layer of the cloud for sustaining PAAS. The platform level is a base for implement the application layer for SAAS applications. Dissimilar types of cloud services demand applications of these resources separately. The infrastructure layer is built with virtualized compute, storage, and network capital. The idea of these hardware resources is meant to offer the elasticity demanded by users. Internally, virtualization realizes automated provisioning of assets and optimizes the infrastructure managing method. The platform layer is for common reason and common usage of the collection of software property. This layer provides users with an environment to build up their appliance, to check task flow, and to manage effecting results and performance. The platform layer must be capable to guarantee users that they have scalability, reliability, and safety protection. In a way, the virtualized cloud platforms serve as a structure middleware between the infrastructure and application layer of the cloud computing. The layer of the cloud architecture is shows below.

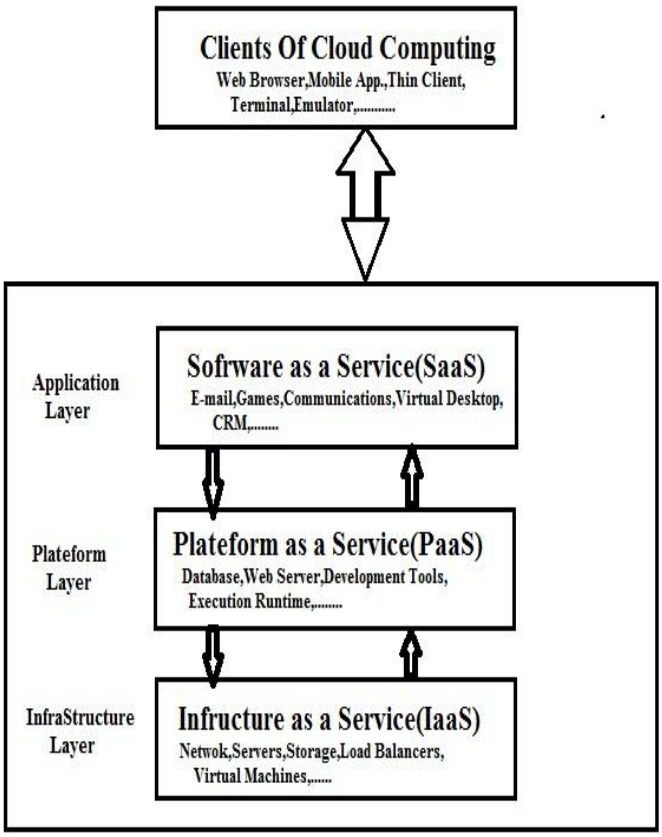

Fig.2 Cloud computing Architecture [12]

The application layer is produced with a group of all required software module for SAAS application. Examination applications in this layer contain daily office management work, such as information recovery, manuscript processing, and calendar and authentication services. The application layer is also heavily used by enterprises in business marketing and sales, consumer relationship management (CRM), financial transactions, and supply chain management. It should be noted that not all cloud services are restricted to a distinct layer. Several applications may concern capital at mix layers. After all, the three layers are built from the bottom up with a dependence relationship.

CONCLUSIONS

In this research paper we have discussed Data Canter Model in Cloud Computing. Cloud computing has an active environment that is flexible, scalable and multi-shared with high ability that gives an inventive form of transportation exposed business. The cloud computing matter of security has become a top priority. This paper discusses the architecture of cloud computing and data security.

ACKNOWLEDGMENT

The credit of accomplish this research goes to our associates for their ethical support. We have grand grateful to our supervisor for hopeful us to write this paper.

REFERENCES

[1]. Brian Hayes. 'Cloud computing'. In: Commun.ACM 51.7(2008), pp.9–11issn:0001-0782.doi: http://doi.acm.org/10.1145/1364782.1364786.URL:http://portal.acm.org/citation.cfm?doid=1364782.1364786

[2]. Colin Ho. Apache flaw opens systems up to attack English.ZDNetUK.Mar.2010.url:http://www.zdnet.co.uk/news/security-threats/2010/03/08/apache-flaw-pens-systems-up-to-attack-40077943/.

[3]. Daniel Nurmi, Rich Wolski et al. 'The Eucalyptus Open-Source Cloud- Computing System'. In: CCGRID '09: Proceedings of the 2009 9th IEEE/ACM International Symposium on Cluster Computing and the Grid.ashington, DC, USA: IEEE Computer Society, 2009, pp. 124–131. ISBN:978-0-7695-3622-4.doi: . http://dx.doi.org/10.1109/CCGRID.2009.93

[4]. Dan Hubbard, Michael Sutton et al. Top Threats to Cloud Computing v1.0.Tech. rep. V1.0. Cloud Security Alliance, Mar. 2010Url:http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf.

[5]. English. Amazon Web Services LLC. url: http://aws.amazon.com/.

[6]. Meiko Jensen, Nils Gruschka and Norbert Luttenberger. 'The Impact of Flooding Attacks on Network-based Services'. In: ARES '08: Proceedings of the 2008 Third International Conference on Availability, Reliability and Security. Washington, DC, USA: IEEE Computer Society, 2008, pp. 509–513.isbn:978-0- 7695-3102-1.doi: http://dx.doi.org/10.1109/ARES.2008.16.

[7]. Meiko Jensen, Jorg Schwenk et al. 'On Technical Security Issues in Cloud Computing'. In: Cloud Computing, IEEE International Conference on 0 (2009), pp.109–116.doi: http://doi.ieeecomputersociety.org/10.1109/CLOUD.2009.60.

[8]. Philippa J. Broadfoot and Andrew P. Martin. A Critical Survey of Grid Security Requirements and Technologies. Tech. rep. PRG-RR-03-15. Wolf- son Building Oarks Road Oxford OX1 3QD: Oxford University Computing Laboratory, 2003.urlhttp://www.comlab.ox.ac.uk/files/930/RR-03-15.ps.gz.

[9]. Phil Wong. Conversations about the Internet #5: Anonymous Facebook Employee. English. The Rumpus. Jan. 2010. url: http://therumpus. net / 2010 / 01 / conversations - about - the - internet - 5 - anonymous - facebook-employee.

[10]. Siani Pearson. 'Taking account of privacy when designing cloud comput- ing services'. In: CLOUD '09: Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing. Washington, DC, USA: IEEE Computer Society, 2009, pp. 44–52. isbn: 978-1-4244-3713-9.doi: http://dx.doi.org/10.1109/CLOUD.2009.5071532.

[11]. Thomas Ristenpart, Eran Tromer et al. 'Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds'. In: 16th ACM Conference on Computer and Communications Security CCS'09. Nov. 2009.

[12]. Odunayo O. Owopetu, Private Cloud Implementation and Security Using EUCALYPTUS and XEN Frameworks.