Security Issues in Cloud Computing-A perspective view

Swaathi.V[1] **Sanjana Raj[2]** **Prithvi.G.I[3]**

[1]Dept. of ISE,BMSIT,swaathiv@yahoo.co.in,9740030055

[2]Dept. of ISE,BMSIT,sanjana.raj11@gmail.com,9620049507

[3]Dept. of ISE,BMSIT,prithvi.gi@gmail.com,9945416121

Abstract: **This paper deals with the solutions to the security, privacy, compliance and vendor lock-in problems and help advance the adoption of cloud computing. Cloud computing is a synonym for distributed computing over a network. Development and advancement in this field is exceptional. It is used in all sorts of industries and educational institutions. The most commonly known example of cloud computing is owned by "*Google*". The Google apps such as Google play, Google maps, Google group, Gmail, Google search engine and more that are made available to the user, makes the task much simpler. Every powerful tool or technology has its own disadvantages. Control and unreliability, security privacy and compliance, compatibility, contracts and vendor lock-ins are some of the grave problems we face today. In this paper we consider different situations and improvise on how it is possible to use cloud computing more efficiently considering the technical aspects, data privacy, security, safety and economic conditions. Here, we strive to provide a better understanding of the cloud concept and in-depth topics pertaining to cloud to identify important research issues in this burgeoning area of computer science.**

Keywords: **Cloud Computing, Restraints, Security issues, API, PKI, SLA, CSA.**

I. INTRODUCTION

Cloud computing can also be called as a colloquial expression used to describe a variety of computing concepts and systems that involve a large number of computers connected through a real time communication network, typically the internet. It is so advanced that it is in itself a jargon term. Cloud computing is not only used in large technical companies but also applicable in schools and campaigning companies as it provides an efficient and low cost option for using high end computing systems.

AFFILIATED TECHNOLOGIES

1. Grid Computing- It is defined as interconnected computer systems where the machine uses resources collectively. Grid computing consists of one main computer that distributes information and tasks to a group of networked computers to accomplish a common goal. This technology, unlike cloud computing, does not provide a platform for the end users to interact. What distinguishes grid computing from other conventional high performance computing systems such as cluster computing is that grids tend to be more loosely coupled, heterogeneous and geographically dispersed.

2. Virtualization- It introduces a layer between hardware and operating system. Virtualization creates a virtual version of resources, such as, operating system, storage devices, servers, etc. where the framework divides it into many execution environment. Virtualization allows us to enable today's x86 computers to run multiple applications which are deployed faster and are more efficient.

We promote Cloud Computing over other conventional methods due to its flexibility, disaster recovery, automatic software update, free capital expenditure, increased collaboration, work from anywhere, document control, competitiveness, environment friendly and many more.

II. TYPES OF CLOUD

1. Public cloud-In computing infrastructure, the public cloud is hosted by a cloud vendor that is set up in the vendor's premises. Public cloud is constructed using pooled, shared physical resources. It offers ultimate scalability, cost effectiveness, utility style costing, reliability and more. A few examples of public clouds are Amazon Elastic Cloud Compute (EC2), Google App Engine, Blue Cloud by IBM and AZURE services Platform by Windows.

2. Private cloud- It is the term used to describe a cloud computing platform within the corporate firewall, which is controlled by the IT department. Private clouds are more expensive and more secure than cloud computing.

3. Hybrid cloud- It includes the benefits of both public and private cloud infrastructures. In other words, some critical data resides in the enterprise's private cloud while other data is stored and accessed from a public cloud.

III. CLOUD INFRASTRUCTURE

The three fundamental cloud computing service models go hand in hand shown in fig1.

IaaS - Infrastructure as a Service includes offerings such as virtual server space, bandwidth, IP addresses and load balances. Physically, the pool of hardware resources is taken from a multitude of distributed network servers, all of which is maintained by the cloud provider. Client, on the other hand, is given access to the virtualized components in order to build their own IT platforms.

SaaS - Software as a service describes any cloud service where consumers are able to access software applications over the internet. The applications are hosted in "the cloud" and can be used for a wide range of tasks for both individuals and organizations. Google, Twitter, Facebook, Flicker are all examples of SaaS with users able to access the services via any internet enabled device.

PaaS - Platform as a service is a category of cloud computing that provides a platform and environment to allow developers to build applications and services over the internet. PaaS services are hosted in the cloud and accessed by users simply via their web browsers and also allows users to create software applications with the help of tools supplied by the provider.

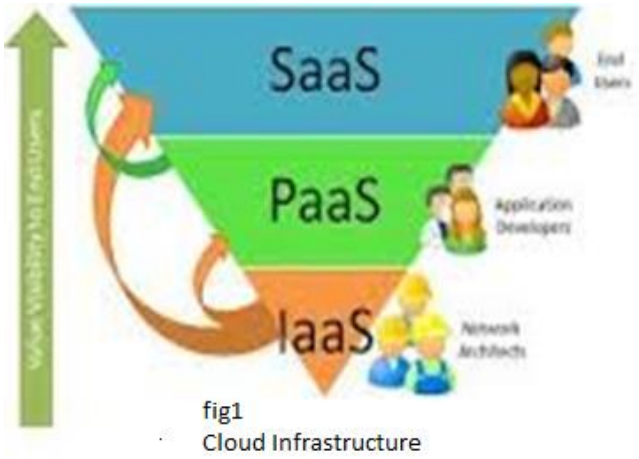

fig1
Cloud Infrastructure

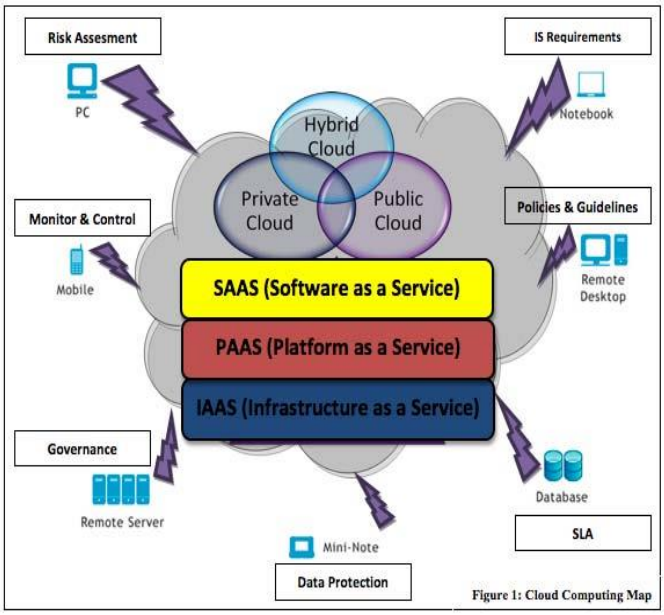

Figure 1: Cloud Computing Map

The main benefits of cloud computing : globalizes your workforce, streamline process i.e. getting more work done in less time with less people, monitoring projects more effectively, achieving economies of scale and making development possible for "non experts".

IV. RESTRAINTS OF CLOUD COMPUTING

Every powerful tool or technology has its own constraints. Our concentration is towards privacy and compliance, contracts and vendor lock-in problems. There is a major hindrance when it comes to security. The vendor of the cloud must make sure that the customer does not face any problems such as loss of data or data theft. There is a possibility where a malicious user can penetrate the cloud by impersonating the cloud user, there by interfering with the entire cloud, thus affecting many customers using it. In cloud, existing vulnerabilities, threats and associated attacks raise several security concerns. Vulnerabilities in cloud can be defined as loopholes in the security architecture of cloud, which can be exploited by an adversary by using sophisticated techniques to gain access to the networks

and other infrastructure resources. Some of the problems (shown in fig2) we deal with are

1. Data Integrity

2. Data Theft

3. Privacy Issues

4. Infected Application

5. Data Loss and Leakage

6. Security on Vendor level-unauthorized access to management interface

7. Data Location-vulnerabilities in virtualization

8. Security on User Level-abusive use of cloud computing interfaces and API's

fig2
Cloud security

Security basically means protection from harm and any vulnerable assets. The same concept is seen in cloud computing. A large multinational company should own a cloud rather than taking it on rent and a small low-budget company should rent a cloud rather than owning it.

1. Account Traffic Hijacking:

It can be resolved by secure disposal of data, encryption key management, providing user id credentials, remote user multifactor authentication, user access policy and audit logging/intrusion detection. Audit logs are needed to record user and system activities, exceptions and information security events, regulatory and legal agreements, record of all changes made to recipient objects to assist in future investigations and access control monitoring.

2. Insecure Interfaces and Application Programming Interface (API):

This threat can be overcome by providing a secure platform for the application and maintaining data security and integrity. By data integrity, we mean maintaining and assuring the accuracy, consistency of data and correctness of data over its entire lifecycle. API provides protocols on how the software components interact with each other. API is a library that includes specifications for routines, data structures, variables and object classes. Social networking sites and blog sites are a few examples of API's.

3. Malicious Insiders:

A malicious insider is an adversary who operates inside the trusting computing base. He is a rogue administrator who attacks the organizational security. To counter this threat by data governance (ownership/stewardship), facility security (off-site authorization), information security i.e. policy enforcement and segregation of duty, deploy integrity protected virtual machine monitors and introducing third party audits.

V. SOLUTIONS

1. Public Key Infrastructure (PKI) - It is a platform that enables users to exchange and manage data securely in an unsecure public network through the use of public and private cryptographic key pair that is obtained and shared through a trusted authority (shown in fig3).The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. PKI help overcome security issues in cloud computing by providing certification authority (CA), registration authority (RA), validation authority (VA) and helps protect confidentiality and authentication.

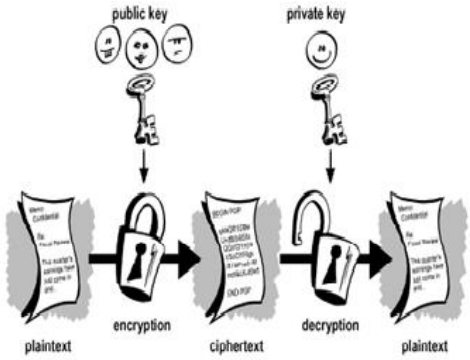

fig3
Public key
infrastructure

To avoid vendor-level and user-level data misuse, we can implement PKI management system that mitigates unauthorized security breach.

PKI also provides an interface for Smart Metering (shown by fig4) by providing digital signatures without opening holes in existing firewalls. This helps in transparently identifying and authenticating users. It also provides signed audit trails which maintains and monitors the access logs and operations performed during a given period of time. It provides appropriate tools to detect security violations, performance problems and flaws in applications.

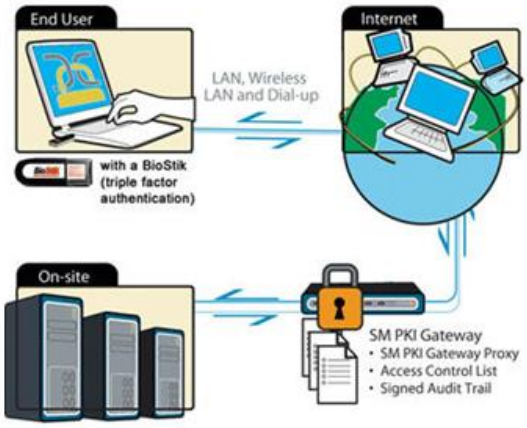

fig4
Smart Metering of PKI

A number of products are offered that enable a group of companies to implement a PKI. A few PKI leaders are RSA, VeriSign, GTE Cyber Trust, etc.

2. Service Level Agreement (SLA) - It is a legally negotiated agreement between cloud consumers and providers. SLA provides a unique combination of business-driven application scenarios and advanced research in the area of service level agreements for clouds and service oriented infrastructure. It pools together information into a single contracted service document that clearly states metrics, responsibilities and expectations to ensure that neither party can plead ignorance in case of an issue. Most SLAs also leave room for annual re-visitation so that it is possible to make changes based on new information.

In today's world, cloud computing technology is so advanced that it plays a significant role in IT. By providing a unique association called the Cloud Security Alliance (CSA), the security breaches are handled.

3. Cloud Security Alliance (CSA)

The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security assurances within Cloud Computing.

The CSA STAR is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings.

To rid off the security problems we are facing such as data integrity, data loss and leakage, we can take the help of CSA by considering the guidelines provided. CSA strives to provide a secure environment for the cloud users and vendors to function effectively. The CSA leads a number of on-going research initiatives through which it provides white papers, tools and reports to help companies and vendors secure cloud computing services. With data being the new currency, the control of trust in the cloud is ever more significant. The CSA updates Certificate of Cloud Security Knowledge (CCSK) that brings out best practice guidelines to IT professionals and provides a consistent way of deploying Cloud Security. CSA furthers global transparency efforts to serve the rapid growth of IT.

VI. FUTURE OF CLOUD

The new era of Cloud Computing has many on-going researches such that an organization can take the role and responsibilities of a Cloud broker, to control source,

to implement and manage multiple Cloud services. This is shown by fig6.

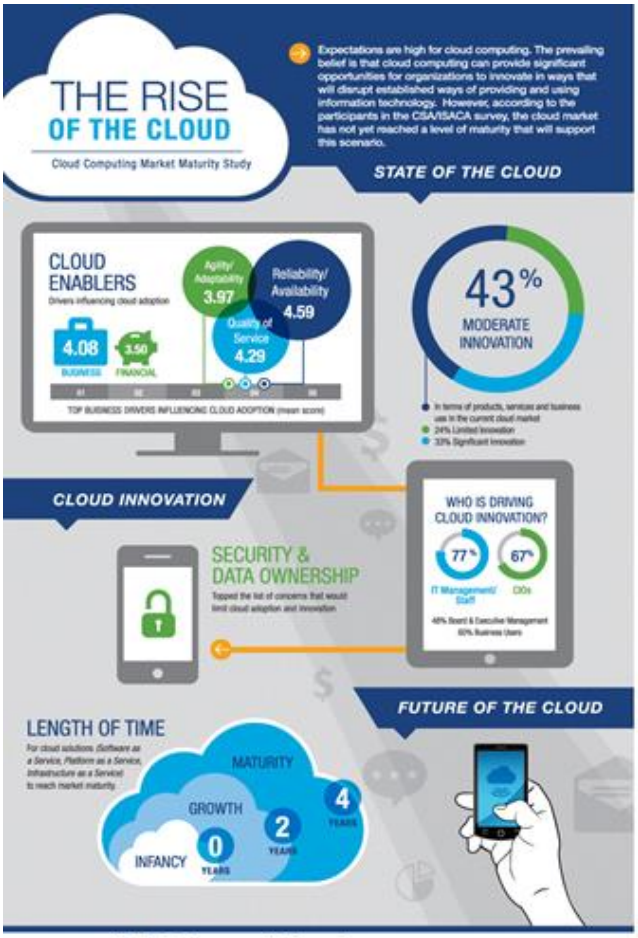

fig6:Future of Cloud

With global customers placing premium on vendors having intellectual property assets, we should strive to create platforms, networks, applications and security looking for best practices.

LATEST DEVELOPMENTS

One of NSE's top priorities today is cloud computing. International Business Machines Corp. (IBM) won a federal cloud computing contract with a maximum value of $1 billion, its largest such agreement with the U.S. government.

Organizations that deal with Security Issues in Cloud Computing

1. DMTF- Distributed Management Task Force

2. OCDA- Open Data Centre Alliance

3. SDO- Standard Developing Organization

4. ISC- International Standardization Council

5. RAISE forums-Regional Asia Information Security Exchange

VII. CONCLUSION

As Cloud Computing provides an effective and efficient way of storing information, it is the most upcoming and fast growing technology in today's IT world. The culmination of Cloud economics will supply strategic resolutions for business and financial market. Due to the weightage Cloud Computing holds, ensuring it provides a secure environment and developing the existing solutions for the betterment of the technology is our ultimate objective in this paper.

VIII. ACKNOWLEDGEMENT

We sincerely thank our Principal,(BMSIT),Dr Rajasimha Makaram, HOD, (Dept. of ISE) and professors for giving us this opportunity to put forth our ideas through this paper.

IX. REFERENCES

[1]. Pradeep Kumar Tiwari and Dr. Bharat Mishra, "Cloud Computing Security Issues, Challenges and Solution", International Journal of Emerging Technology and Advanced Engineering, Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[2].http://www.x500standard.com/index.php?n=Ig.KM

[3].http://www.x500standard.com/index.php?n=Ig.WPKI

[4] Ms. Heena Kharche and A step towards cloud trust by Mr. Deepak Singh Chouhan, Building Trust In Cloud Using Public Key Infrastructure, Vol. 3, No. 3,2012, International Journal of Advanced Computer Science and Applications (IJACSA).

[5].http://www.keynectis.com/en/manage-your-assets-securely-in-the-cloud

[6].http://www.ejbca.org/services-va.html

[7].http://www.webopedia.com/TERM/S/Service_Level_Agreement.html

[8].http://www.sla.org/

[9].http://www.cio.com/article/128900/SLA_Definitions_and_Solutions

[10].http://www.sei.cmu.edu/library/abstracts/reports/12tn001.cfm

[11].http://www.redbooks.ibm.com/abstracts/redp5024.html

[12].http://www.pwc.com/

[13].http://www.interoute.com/search/node/paas

[14].http://ieeexplore.ieee.org/xpl/download Citations

[15].http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5716422&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5716422

[16].http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6334973

[17].http://www.google.com/apps/intl/en/terms/sla.html

[18].http://go.microsoft.com/fwlink/?LinkID=219472&clcid=0x409

[19].http://csrc.nist.gov/publications/nistbul/itl97-03.txt

[20]http://www.onlineconversion.com/length_common.htm

[21].http://www.infosecisland.com/

[22].http://folding.stanford.edu/

[23]. Cloud Service Alliance, Privacy Level Agreement Working Group, Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union, February 2013

[24].http://www.pwc.com/ - International journal of next generation technology

[25].http://perpetualinnovation.net/ojs/

[26].http://www.businesswire.com/news/home/20130619005581/en/2013-Future-Cloud-Computing-Survey-Reveals-Business

[27].http://www.business-standard.com/article/news-ians/indian-it-industry-to-build-next-generation-enterprises-113082201146_1.http

[28] Cloud Service Alliance, Top Threats Working Group, The Notorious Nine, Cloud Computing Top Threats, February 2013.

[29].http://help.outlook.com/en-in/140/ee845533.aspx

[30].http://docs.oracle.com/cd/E24191_01/custom/deploy/audit_trail.html

[31].http://ace.apache.org/dev-doc/analysis/auditlog-analysis.html

[32].http://www.interoute.com/what-paas

[33].http://www.interoute.com/what-saas

[34].http://www.informationweek.com/security/attacks/10-best-ways-to-stop-insider-attacks/232602440

[35] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya, Avi Patel and Muttukrishnan Rajarajan, A survey on security issues and solutions at different layers of Cloud computing, Published online: 13 October 2012, © Springer Science+Business Media New York 2012.

[36].https://www.google.co.in/search?biw=1280&bih=720&q=csa+standards&revid=804026969&sa=X&ei=ZAY0UomDBIL8rAfDtYAw&ved=0CGMQ1QIoAA

[37].http://directories.csa-international.org/

[38].http://www.csa.com/

[39].https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=gts-LITS-desktop-cloud-NA&S_PKG=ov6247&csr=agus_scecloudsnotequal-20120517&cm=k&cr=google&ct=103JK01W&S_TACT=103JK01W&ck=advantages_of_cloud_computing&cmp=103JK&mkwid=sgo45bX0B-dc_34899422271_432r5u7605

[40].http://www.verio.com/resource-center/articles/cloud-computing-benefits/

[41].http://www.salesforce.com/uk/socialsuccess/cloud-computing/why-move-to-cloud-10-benefits-cloud-computing.jsp

[42].http://docs.openstack.org/api/openstack-identity-service/2.0/content/GET_getUserCredential_v2.0_users__userId__OS-KSADM_credentials__credential-type__.html

[43].http://www-03.ibm.com/systems/virtualization/

[44].http://www.vmware.com/virtualization.html

[45].www.webopedia.com

[46].http://www.springer.com/computer/communication+networks/journal/10723

[47].http://enterthegrid.com/