Cloud Computing & Resolving its Security Issues

Shashank Gupta
Department of Computer Science & Engineering
TCET,Indore
shashankg125@gmail.com

Surabhi Prakash
Department of Computer Science & Engineering
TCET,Indore
prakash.surabhi25@gmail.com

Vaishnavi Isasare
Department of Computer Science & Engineering
TCET,Indore
isasare.vaishnavi@gmail.com

Abstract **-- Cloud computing is a metaphor used by Technology or IT Services companies for the delivery of computing requirements as a service to a heterogeneous community of end-recipients. As cloud computing is achieving increased popularity, concerns are being voiced about the security issues introduced through adoption of this new model. The complexity of security is greatly increased when data is distributed over a wider area and today client privacy, confidentiality and security are central to us. In this paper we have studied the specific standards for security or data privacy in cloud computing & propose a security architecture for more consistent security and monitoring of cloud services specifically for safe delivery & modification of client data. For every session to access the cloud the enterprise clients will be authenticated & authorised before presenting itself to cloud service provider. Here, we try to resolve the problems by giving some solutions and their impact on adoption.**

1. Introduction:

After the concept of Cloud Computing was proposed to public by the Google and though many years of accumulation and sustained exploration, this new idea of IT software hasbecome the mainstream, recognized voice---The core of cloud computing is all sorts application platform and information resources connected by Internet as well as cloud infrastructure--based supplied to users(Enterprises or Individuals). The related applications and resources was removed from portable desktop or hardware-software intolarge cloud computing centers, which is delivered as software as a service (SaaS), platform as a service (PaaS), Infrastructure as a service (IaaS),to provide all kinds of services on-demand.[4]

1.1. Fundamental models of Cloud:

1.1.1. SaaS

Software as a service (SaaS) model has similar meanings to the application service provider or hosted software. SaaS--cloud computing-based and lies on WEB services—contributes the easy operation, interfaces and the technology of data storage and exchange, and other Business process. With the use of SaaS, cloud Users no need to buy as many application software as before and no need for software maintenance. Cloud users via the Internet or off-line operate the local data storage. SaaS makes it is possible for the users to choice the software upon on their own demand (software on-demand). This new model delivers software as utility services and charges on a pay-per-use basis, similar to the way a utility company charges for electricity. It not only can help enterprises reduce cost, which is investment in pure hardware and software, but also can prevent the needs for purchasing,building and maintenance of infrastructure and applications.

1.1.2. PaaS

Platform as a services (PaaS) was widely defined as the model that sends operating system and related services internet-based and no need download or setup. PaaS is the application and extension of software as a service.

1.1.3. IaaS

Infrastructure as a service (IaaS) also known as Cloud infrastructure services. Computer infrastructure “as-a-service”,billed on a utility basis and consumption [18].Typically as a virtualized environment to provide services, cloud computing applications, which can be component of as a cloud platform. IaaS means virtual private offerings, so, the users can update its own IaaS module to the cloud platform evolved from SaaS for sale.

1.2. Benefits of Cloud Computing:

Compared with the traditional software theory and application, cloud computing have a lot of

benefits cannot be replaced and representation of the revolutionary ideal. So the development of cloud computing is attracting more and more attention and inspiring. Cloud computing influences on the way people work and life style definitely in upcoming decades. Clients in future via the internet enjoy the services more comfortable but pay less. Cloud computing will shift the economic landscape of information and communication technologies, especially IT trade and ERP, to the same magnitude as did the first wave of the Internet.

But undoubtedly, the development and applications of cloud computing is still facing plenty of questions such as data protection and read, cloud protocol, cloud safety and communication between cloud vendors and users to be solved.

2. Security in Cloud Computing:

Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility (like the electricity grid) over a network (typically the Internet).

Cloud computing has powerful attractions for the organization. It offers instant access to an infinitely flexible computing resource and the ability to make major cost savings through outsourcing. Yet for many organisations, the final barrier to adopting Cloud computing is whether it is sufficiently secure.

SaaS (software as a service) and PaaS (platform as a service) providers all trumpet the robustness of their systems, often claiming that security in the cloud is tighter than in most enterprises. But the simple fact is that every security system that has ever been breached was once thought infallible.

At the heart of cloud infrastructure is this idea of multi-tenancy and decoupling between specific hardware resources and applications. In the jungle of multi-tenant data, one need to trust the cloud provider that their information will not be exposed.

For their part, companies need to be vigilant, for instance about how passwords are assigned, protected and changed. Cloud service providers typically work with numbers of third parties, and customers are advised to gain information about those companies which could potentially access their data.

As with most SaaS offerings, the applications offering are constantly being revised, a fact which raises more security issues for customers. Companies need to know, for instance, whether a software change might actually alter its security settings. For every update we review the security requirements for every user in the system.

However, according to Datamonitor's Trifković, the cloud is still very much a new frontier with very little in the way of specific standards for security or data privacy. In many ways he says that cloud computing is in a similar position to where the recording industry found itself when it was trying to combat peer-to-peer file sharing with copyright laws created in the age of analogue.

Many are concerned that cloud computing remains at such an embryonic stage that the imposition of strict standards could do more harm than good.[14]

2.1. Local law and jurisdiction where data is held

Possibly even more pressing an issue than standards in this new frontier is the emerging question of jurisdiction. Data that might be secure in one country may not be secure in another. In many cases though, users of cloud services don't know where their information is held. Currently in the process of trying to harmonise the data laws of its member states, the EU favours very strict protection of privacy, while in America laws such as the US Patriot Act invest government and other agencies with virtually limitless powers to access information including that belonging to companies.[13]

Cloud computing is facing trouble in seeping within the US federal lines because the US Federation doubts the security of their confidential data logs.[15]

Cloud computing is surely taking the world by rage but as far as the US government is concerned, they still have their reservations in completely using cloud for their data management. Vivek Kundra, the White House's chief information officer was a strong advocate of cloud computing but it appears that the US government will wait for another couple of years before entrusting their data to cloud.[15].He believes that cloud computing can open horizons that would prove to be wondrous for the IT industry.

However, the US government's priority is security and for this they are hesitant in allotting the cloud computing companies, the door keys of their data centers which are highly confidential. They say that Contractors like Amazon, Google and Lockheed Martin are known suppliers of cloud but despite that, the liability of getting their confident data in danger, still exists. These three companies have made it big by providing cloud services in several spheres of life. But the US federation does not want to go under pressure and bear any violent consequences later.[15]

An example of the US security leak is the attack on Pentagon when 24,000 confidential files were hacked. Such discrepancy occurred in a manual situation however; on net too they will be able to make it work one way or the other.

"When done with the proper considerations and planning, cloud computing will be a very effective and efficient tool," Ms. Takai said.[15]

3. Background

Published in E -Business and E -Government (ICEE), 2011 International Conference on **"**Overview and Analysis of Cloud Computing Research and Application" by Yizeng Chen , Xingui Li and Fangning Chen (School of Management Shanghai University, SHU Shanghai, China),this paper aims to the current cloud computing research and application and analyzes the characteristic of cloud computing.[4]

White Paper on "Ensuring Security-The last barrier to Cloud Adoption (Cable & wireless worldwide) published in March 2011 examines the perceived risks, assesses whether they are justified, and the technology and measures that can make the Cloud's 'virtual' security a reality."[6]

The paper appeared in Communication Software and Networks (ICCSN), May 2011 IEEE 3rd International Conference on "Cloud computing security threats and responses" by Farzad Sabahi Faculty of Computer Engineering in Azad University, Iran summarizes availability, and security issues for cloud computing (RAS issues), and propose feasible and available solutions for some of them.[11]

Appeared in Services Computing, 2009. SCC '09. IEEE International Conference on"Cloud security issues" by Balachandra Reddy Kandukuri , Ramakrishna Paturi V from Advanced Software Technologies International Institute of Information Technology, Pune proposed that there has to be a standardized way to prepare the SLA irrespective to the providers. This can help some of the enterprises to look forward in using the cloud services. In this paper, they put forward some security issues that have to be included in SLA(Service Level Agreement).[7]

After the concept of Cloud computing--the Revolutionary development and progress in IT industry-- was born in Google, the IT software and services vendors, universities, enterprises, etc, join in the process of research and application of cloud computing.

Cloud computing technology is not an innovation, but the integration of past technology, even also the future of the software industry model (software 10.0). On the definition of cloud computing has not yet formed a unified understanding in academia, but what has generally been accepted is that cloud computing is the developing result of Grid Computing, Distributed Computing, Parallel Computing, Utility Computing, Network Storage Technologies, Virtualization,Load Balance, etc traditional computer technology. It is designed to provide users with cloud architecture nodes and via the Internet or intranet to integrate the number of relatively low-cost computer entities into one system with powerful computing capabilities. With the help of software of architecture (SOA), SaaS, PaaS, IaaS, management service supply (MSS) and other advanced software models, this powerful Cloud computing capability distributed to the cloud users' (individual or corporate) hands.

The core vision of Cloud Computing is to continuously improve the compute power of "cloud", thereby reducing the processing burden and the cost of cloud users, ultimately to simplify the cloud users into an simple Input and Output devices (I\O Infrastructure), and to enjoy the powerful "cloud" computing capability On-Demand.

These issues which discussed in the paper are the main reasons that cause many enterprises which have a plane to migrate to cloud prefer using cloud for less sensitive data and store

important data in their own local machine.

4. Security challenges in Cloud :

Security – The main Barrier in cloud computing

One of the world's largest technology companies, Google, has invested a lot of money into the cloud space, where it recognises that having a reputation for security is a key determinant of success. "Security is built into the DNA of our products," says a company spokesperson. "Google practices a defense-in-depth security strategy, by architecting security into our people, process and technologies".

Google was forced to make an embarrassing apology in February when its Gmail service collapsed in Europe, while Salesforce.com is still smarting from a phishing attack in 2007 which duped a staff member into revealing passwords.[13]

While cloud service providers face similar security issues as other sorts of organisations,analysts warn that the cloud is becoming particularly attractive to cyber crooks. The richer the pot of data, the more cloud service providers need to do to protect it.

4.1. Security-as-a- service

In Cloud environment the security provided by customers using cloud services and the cloud service providers(CSPs).Security-as-a-service is a security provided as cloud services and it can provided in two methods: In first method anyone can changing their delivery methods to include cloud services comprises established information security vendors. The second method Cloud Service Providers are providing security only as a cloud service with information security companies.Almost all the security companies, anti-malware vendors involved in the delivery of SaaS with regard to email filtering and so on.

4.2. Authentication

In the cloud environment, the primary basis for access control is user authentication and access control are more important than ever since the cloud and all of its data are accessible to all over the Internet. Trusted Platform Module (TPM) is a widely available and stronger authentication than username and passwords. Trusted Computing Groups (TCG's) is IF-MAP standard about authorized users and other security issue in real-time communication between the cloud provider and the customer. When a user is reassigned or fired, the customer's uniqueness management system can report the cloud provider in real-time so that the user's cloud access can be revoked or modified within seconds. In cloud any fired user is logged, they can be immediately disconnected.

Trusted Computing enables authentication of client nodes and other devices for improving the security in cloud computing. The frequently targeted attack is authentication in hosted and virtual services. The secure mechanisms are used to the authentication process for frequent target of attackers by different ways to authenticate users based on different information know by the user.

4.3. Service Provider Security Issues

The public cloud computing surroundings offered by the cloud supplier and make sure that a cloud computing resolution satisfies organizational security and privacy needs. The cloud supplier to provision the safety controls necessary to safeguard the organization's information and applications, and additionally the proof provided regarding the effectiveness of these controls migrating organizational information and functions into the cloud.

4.4. Identity and access management

Identity and Access Management (IAM) features are Authorization, Authentication, and Auditing (AAA) of users accessing cloud services. In any organization "trust boundary" is mostly static and is monitored and controlled for applications which are deployed within the organization's perimeter. In a private data center, it managed the trust boundary encompasses the network, systems, and applications. And it is secured via network security controls including intrusion prevention systems (IPSs), intrusion detection systems (IDSs), virtual private networks (VPNs), and multifactor authentication.

With cloud computing, the organization's trust boundary will become dynamic and the application, system, and network boundary of an organization will extend into the service provider domain. Application security and user access controls will compensate for the

loss of network control and to strengthen risk assurance.Strong authorization, authentication based on claims or role, trusted sources with user activity monitoring, identity federation , accurate attributes, single sign-on (SSO), and auditing.

4.5. Privacy

Privacy is the one of the Security issue in cloud computing. Personal information regulations vary across the world and number of restrictions placed by number of countries whether it stored outside of the country. For a cloud service provider, in every jurisdiction a single level of service that is acceptable. Based on contractual commitments data can store within specific countries for privacy regulations, but this is difficult to verify.

In Private and confidential customer data fast rising for the consequences and potential costs of mistakes for companies that handle. But professionals develop the security services and the cloud service privacy practices. An effective assessment strategy must cover data protection, compliance, privacy, identity management, secure operations, and other related security and legal issues.

4.6. Securing Data in Transmission

Encryption techniques are used for data in transmission. To provide the protection for data only goes where the customer wants it to go by using authentication and integrity and is not modified in transmission. SSL/TLS protocols are used here.

In Cloud environment most of the data is not encrypted in the processing time.But to process data, for any application that data must be unencrypted. In a fully homomorphism encryption scheme advance in cryptography, which allows data to be processed without being decrypted. To provide the confidentiality and integrity of data-in-transmission to and from cloud provider by using access controls like authorization, authentication, auditing for using resources, and ensure the availability of the Internet-facing resources at cloud provider. Man-in-the-middle attacks is cryptographic attack is carried out when an attacker can place themselves in the communication's path between the users. Here, there is the possibility that they can interrupt and change communications.

4.7. User Identity

In Organizations, only authorized users across their enterprise and access to the data and tools that they require, when they require them, and all unauthorized users are blocked for access. In Cloud environments support a large enterprise and various communities of users, so these controls are more critical. Clouds begin a new level of privileged users working for the cloud provider is administrators

4.8. Separation between Users

One of the most important cloud concerns issue is separation between a cloud provider's users to avoid intentional or inadvertent access to sensitive information. In a cloud Environment, provider use virtual machines (VMs) and a hypervisor to separate cloud customers.

4.9. Cloud legal issues

A cloud provider has practices and strong policies that address regulatory and legal issues, to inspect cloud provider policies and practices to ensure their adequacy each customer must have its legal and regulatory experts. The issues to be considered include auditing, data security and export, data retention and destruction, legal discovery and compliance. In limiting access to data, Trusted Storage and TPM access techniques can play a key role.

4.10. Securing Data-Storage

In Cloud computing environment data protection as the most important security issue. In this issue , it concerns include the way in which data is accessed and stored , audit requirements, compliance , notification requirements , issues involving the cost of data breaches, and damage to brand value. In the cloud storage infrastructure, regulated and sensitive data needs to be properly segregated. In the service provider's data center,protecting data privacy and managing compliance are critical by using encrypting and managing encryption keys of data in transfer to the cloud.

Encryption keys share securely between Consumer and the cloud service provider and encryption of mobile media is an important and often overlooked need. PaaS based applications, Data-at-rest is the economics of

cloud computing and a multitenancy architecture used in SaaS. In other words, data, when stored for use by a cloud-based application or, processed by a cloud-based application, is commingled with other users' data. In cloud computing, data co-location has some significant restrictions. In public and financial services areas involving users and data with different risks. The cloud-wide data classification will govern how that data is encrypted, who has access and archived, and how technologies are used to prevent data loss.

At the cloud provider, the best practice for securing data at rest is cryptographic encryption and shipping self encrypting is used by hard drive manufacturers. Self-encrypting provides automated encryption with performance or minimal cost impact.

5. Proposed Solution

Cloud computing puts your data outside of your organization. Also when we use a cloud computing service, we are limiting yourself to the amount of advanced security tools that you can put on the system. There are also other issues to consider. We have little control over how much audit information is collected. For example, we likely do not have access to failed log-in attempts, so we cannot proactively look for attack reconnaissance. Likewise, while we may maintain ownership of your own data, we do not likely own all of the access log data. That potentially creates legal problems. For example, if someone does illicitly access our information, we might need to get a court order to see where they are coming from. If however we maintained your data internally, you would have instant access to all of this information.

The problem was that the users or the clients are not satisfied with the data security on cloud service provider. Clients want more security of data when they upload their confidential data on cloud. However, if our organization with a great deal of intellectual property, believe that our data is valuable, and intend to implement more than basic security measures, we probably need to maintain your own data infrastructure. We can however review cloud computing providers and see if they allow for the implementation of the security countermeasures we believe are necessary.

The Cloud computing security concept we propose will hand over ultimate control to the customer in order to meet their requirements for authentication, authorisation & encryption of resources available through cloud service provider.

- Requirement of an Operating System which will support the architecture of Cloud Computing. If we have such an OS which is made for the Cloud Computing then it will be easy to run Cloud Apps on that OS.
- VPN based (comprising of organisation and service provider) WAN among the client enterprise containing a server which is doing the authentication of internal client who subsequently can avail the services from the Cloud Computing service provider.
- Use of Random Encryption Algorithms so that the intruder or hacker find it difficult to peep into clients personal Data.

6. Conclusion

First, identify the business processes and information requirements associated with those business processes and then build your security services so that they adequately protect these business services from realistic threats and attack vectors - regardless of delivery model.

The challenge then is to identify appropriate technologies and processes to meet these architectural requirements in the implementation across various delivery models to ensure a consistent level of control. It is equally important to ascertain the levels of assurance required of these identified controls, as this may rule out certain delivery models, subject to business risk tolerances.

For too long security has been seen as a blocker and detached from the business, security architecture is the means to bridge this gap and help organisations to take advantage of new technologies within risk tolerances that the business understands and accepts.

7. Future Work:

In future, we can use multiple encryption algorithms for encryption & decryption of data for secure data storage on cloud.

8. References:

[1] Meiko Jensen, Jörg Schwenk, Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", 2009 IEEE International Conference on Cloud Computing

[2] Michael Gregg, "10 Security Concerns for Cloud Computing", Expert Reference Series of White Papers, Global Knowledge, 2010

[3] **"**IBM Point of View: Security and Cloud Computing", Cloud computing White paper November, 2009.

[4] Overview and Analysis of Cloud Computing Research and Application" by Yizeng Chen , Xingui Li and Fangning Chen (School of Management Shanghai University, SHU Shanghai, China).

[5] "Security and high availability in cloud computing environments" , IBM Global Technology Services Technical White Paper ,IBM , June 2011

[6] Ensuring Security-The last barrier to Cloud Adoption (Cable & wireless worldwide) in March 2011

[7] "Cloud security issues" by BalachandraReddyKandukuri,Ramakrishna Paturi V from Advanced Software Technologies International Institute of Information Technology, Pune.

[8] Ronald L. Krutz, Russell Dean Vines "Cloud Security A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, Inc., 2010

[9] Tim Mather, Subra Kumaraswamy, Shahed Latif "Cloud Security and Privacy", O'Reilly Media, 2009

[10] John W. Rittinghouse, James F. Ransome "Cloud Computing: Implementation, Management, and Security" ,CRC Press, 2009.

[11] Cloud computing security threats and responses" by Farzad Sabahi Faculty of Computer Engineering in Azad University, Iran

[12] Top five cloud computing security issues by David Binning, April 2009 http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud- computing-security-issues.htm

[14] Security Zone: Cloud computing puts the spotlight on security architecture by Lee Newcombe,November2010,http://www.computerweekly.com/Articles/2010/11/25/244113/Security-Zone-Cloud-computing-puts-the-spotlight-on-security.htm

[15] Cloud computing is facing trouble in seeping within the US federal lines because the US Federation doubts the security of their confidential data logs. http://cloudtechsite.com/blogposts/us-federation-expresses-doubt-over-use-of-%E2%80%98cloudtechnology%E2%80%99.html