CLOUD COMPUTING: SECURITY ISSUES

IshaMehra[1] , Deepshikha[2],Sachin Singh

Scholar,ccsit,tmu , Scholar,ccsit, tmu

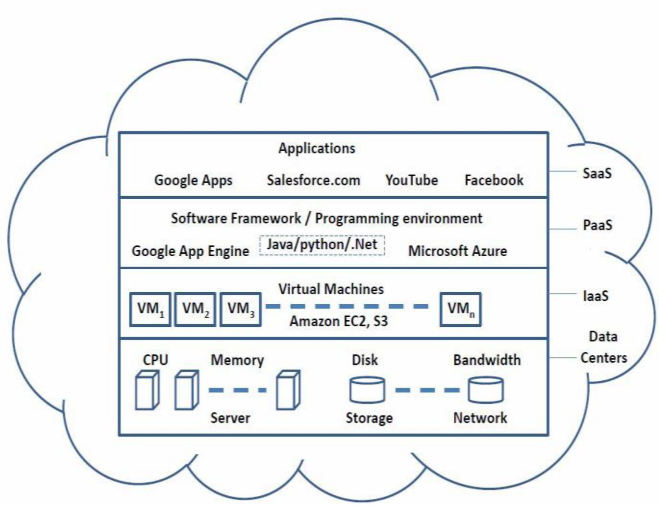
Assistant professor ,ccsit ,tmu
[1] Ishumehra241@gmail.com
[2]deepsb997@gmail.com
[3]sachin.computers@tmu.ac.in

Abstract**: Cloud computing has formed the real & infrastructure basis for tomorrow's computing. Now a days, our global computing infrastructure is fastly moving towards cloud based architecture. Cloud computing is much more than simple internet. Confidentially, Privacy, Integrity Availability, Authenticity are important points for both consumer as well as cloud providers. This paper highlights all the security issues that come from the using of cloud services and we examine more cloud computing system providers about their relevant on privacy and security issues.**

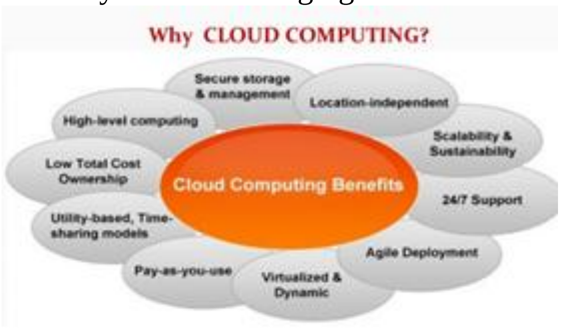
KEYWORD**: Security issues, confidentiality, authenticity, trust, cloud computing, encryption.**

I. INTRODUCTION

The latest idea of cloud computing give enterprise measurability resources supply as a work over the internet and gives a more economic profit to be administer among its users. In past, many organizations had built a costly infrastructure to maintain their routine tasks and it store the data of organization. In early time data was stored in relational databases that located inside server of the organization and then client retrieve that data from server machine. This technique was so expensive because it needed to engage personnel for distribute, handle, keep up the infrastructure. In last days, idea of clusters and grid computing provide a new method for keep the data. It can store the data on clusters and in the form of grid, but they were lightly coupled, heterogeneous and scattered all over the world.



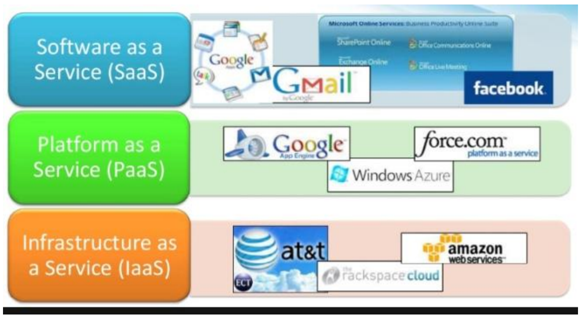
The idea of cloud computing is mainly a modern idea that take birth from clusters and grid computing.There are three types of services are- Software-as-a-services, Platform-as-a-services and Infrastructure-as-a-services. Cloud computing is a that type of infrastructure that provide a business necessity without managing it.



Although at early time, this concept was present only in the academic area, recently Microsoft, Google, Amazon and Salesform.com was transposed it. It diminished the cost of infrastructure and become a new startup to enter the market easier. By this user can access heavy application by a light weight devices like Mobile phones, PCs, PDAs etc. It can deliver common online business applications which are access from server through a web browser.

II. MODELS OF CLOUD COMPUTING

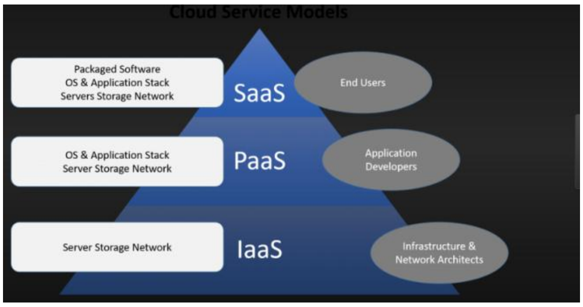
Cloud computing are categories into a three model, namely-Software as a services, Platform as a services, Infrastructure as a services.


Software as a Service (SaaS)
Google
Gmail
facebook
Microsoft Online Services
Platform as a Service (PaaS)
Google App Engine
force.com platform as a service
Windows Azure
Infrastructure as a Service (IaaS)
at&t
amazon web services
rackspace cloud

Software-as-a- services-It is a process in which Application Service Provider provide a different software application over the internet. This makes the customer to get rid of installing and operating the application on own computer and also decrease the large load of software maintenance.

Software as a Service (SaaS)
Google
Gmail
facebook
Microsoft Online Services
SharePoint Online
Exchange Online
Office Communications Online
Office Live Meeting

SAAS vendor advertently takes responsibility for deploying and managing the IT infrastructure and process required to run and manage the full solution. Example- Salesforce.com, Google App.



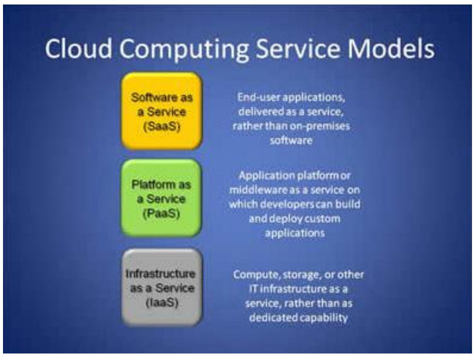
Platform-as-a-services-Pass is the delivery of a computing platform and solution stack as a service without software downloads installation for developers, IT manager or end user. It provides an infrastructure with a high level of integration in order to implement and test cloud application. Its infrastructure does not manage by user but it controls deployed application and possibly their configuration. Example- Force.com, Google App Engine etc.

Platform as a Service (PaaS)
Google App Engine
force.com platform as a service
Windows Azure

Infrastructure-as-a-services-It is refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. In general, the user does not manage the underlying hardware in the cloud infrastructure, but he controls the operating systems, storage and deployed applications.

Infrastructure as a Service (IaaS)
at&t
amazon web services
rackspace cloud

Example-Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.



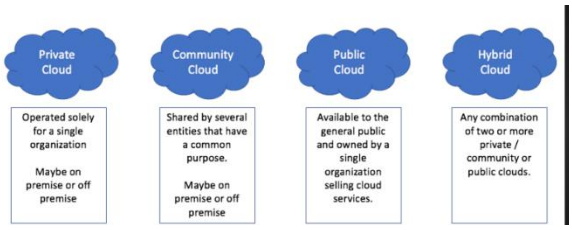
Cloud Computing Service Models

Software as a Service (SaaS) — End-user applications, delivered as a service, rather than on-premises software

Platform as a Service (PaaS) — Application platform or middleware as a service on which developers can build and deploy custom applications

Infrastructure as a Service (IaaS) — Compute, storage, or other IT infrastructure as a service, rather than as dedicated capability

III. CLOUD DEPLOYMENT MODEL



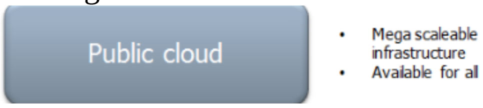
Private Cloud: Operated solely for a single organization. Maybe on premise or off premise

Community Cloud: Shared by several entities that have a common purpose. Maybe on premise or off premise

Public Cloud: Available to the general public and owned by a single organization selling cloud services.

Hybrid Cloud: Any combination of two or more private / community or public clouds.

Public Cloud: Public cloud describe the straight meaning of cloud computing that is available, valuable ways and means, which are accessible on internet from a minor party, which separated assets and charge its clients on the basis of usefulness.



- Mega scaleable infrastructure
- Available for all

Cloud organization is obsessed and achieve by a dealer who advice its retune to public domain. E.g. Google, Amazon, Microsoft offers cloud services via Internet. There are so many profit of using a public cloud model.

Private Cloud: Private cloud is a word used to donate a proprietary computing architecture provisioned services on corporate networks. Big enterprises mainly used this type of cloud computing to permit their private network and information Centre administrators to effectively become in-house 'service providers' catering to customers within the corporation.

Private cloud

- Outsource or own
- Lease or buy
- Separate or virtual data center

Cloud organization is establishing for a particular aggregation and managed by a third party under a service level agreement. Only single organization preferred to operate via corporate cloud. There are so many benefits of using this cloud.

Hybrid Cloud: A hybrid cloud comprises assets from both corporate and public providers will definitely become the demanded choice for enterprises. It is a combination of corporate cloud and public cloud.

Hybrid cloud

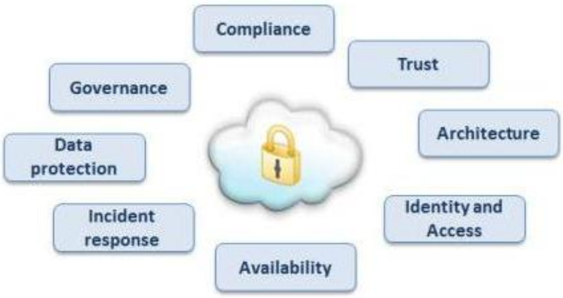
- Combination of two clouds
- Usually private for sensitive data and strategic applications

For example, for general computing enterprise could selects to make habit of external services, and its own data Centre's comprises it own data Centre'. It have so many advantages.

Community cloud :Community clouds shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party, and either hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.A community cloud in computing is a collaborative effort in which infrastructure is shared between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party and hosted internally or externally.

IV. SECURITY ISSUES AND SOLUTION

The problem of security issues are discuss here-



TRUST-Trust between user and the services is the main factor faced by cloud computing today. Customer is never sure about the Service is secured or not, and whether his data is secure from the intruders or not. The customer and Service provider are bound by Service Level Agreement (SLA) document. This is a form of an agreement between the customer and the service provider; it contains the duties of service provider and his future plans. But in some case there are no standards for SLA. Many hard works have been made till now to decide the issues of trust and privacy to determine the security issues in cloud.

CONFIDENTIALLY-Confidentiality means to avoid the exposé of private and crucial information. Since all the information is stored on geologically isolated locations, privacy becomes a huge issue. Numerous methods are second-hand to defend secrecy from which, encryption isthe commonly used method. But it is comparatively a costly method. To conserve confidentiality, a secure cloud storage service is designed that is built upon the public cloud organization and by using cryptographic technique, confidentiality is achieved.

AUTHENTICITY-Integrity is also a main matter faced by cloud computing. It refers to the rude modification of information. As thedata resides in diverse places in a cloud so the access manage mechanism should be very safe and each user must be confirmed as an authentic user. Authentication issues can be handle by using the digital signatures but even after having access to digital signatures a user can't get access and prove the subsets of data. An access control scheme presented by is a decentralized and forceful access control mechanism where the cloud user uniqueness is verified by the cloud without knowing the user's identity before storing information.

ENCRYPTION-Encryption is the most broadly used data securing method in cloud computing. It has many outcomes. It needs layer of computational power. The encrypted data need to be decrypted every time when a query is run so it decreases the Whole database performance. Many methods are now introduce to ensure good encryption in the form of better security or the operations. Data is encrypted using these methods in each cell of a table in cloud. Whenever a user wants to make a query, the query parameters are evaluated against the data stored. The query results are also decrypted by the user not the cloud itself so it increases the whole performance.

KEY MANAGEMENT-When we doing an encryption or decryption, managing a key itself are a big issue. Cloud is storing that key on itself which is a bad option.This may need a little database to store a key locally in a save database. But again that's not a good idea because the purpose forwhich we are shifting our data to clouds will becomeworthless. As by doing so we will need additionalhardware and software resources and the cost issues willalso arise. The only solution to key management may bethrough two-level encryption. This can be veryhelpful to store encryption keys in cloud.

V. Disadvantages of cloud computing

1. *Downtime*

As cloud service providers take care of a number of clients each day, they can become overwhelmed and may even come up against technical outages. This can lead to your business processes being temporarily suspended. Additionally, if your internet connection is offline, you will not be able to access any of your applications, server or data from the cloud.

2. *Security*

Although cloud service providers implement the best security standards and industry certifications, storing data and important files on external service providers always opens up risks. Using cloud-powered technologies means you need to provide your service provider with access to important business data. Meanwhile, being a public service opens up cloud service providers to security challenges on a routine basis. The ease in procuring and accessing cloud services can also give nefarious users the ability to scan, identify and exploit loopholes and vulnerabilities within a system. For instance, in a multi-tenant cloud architecture where multiple users are hosted on the same server, a hacker might try to break into the data of other users hosted and stored on the same server. However, such exploits and loopholes are not likely to surface, and the likelihood of a compromise is not great.

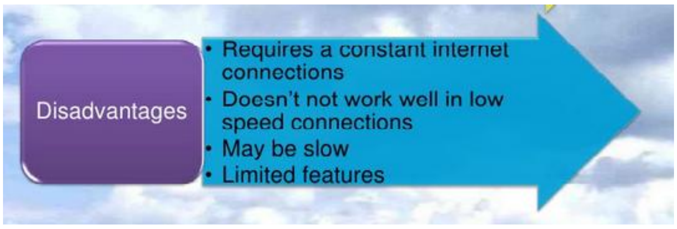
3. *Vendor Lock-In*

Although cloud service providers promise that the cloud will be flexible to use and integrate, switching cloud services is something that hasn’t yet completely evolved. Organizations may find it difficult to migrate their services from one vendor to another. Hosting and integrating current cloud applications on another platform may throw up interoperability and support issues. For instance, applications developed on Microsoft Development Framework (.Net) might not work properly on the Linux platform.

4. *Limited Control*

Since the cloud infrastructure is entirely owned, managed and monitored by the service provider, it transfers minimal control over to the customer. The customer can only control and manage the applications, data and services operated on top of that, not the backend infrastructure itself. Key administrative tasks such as server shell access, updating and firmware management may not be passed to the customer or end user.

It is easy to see how theadvantages of cloud computing easily outweigh the drawbacks. Decreased costs, reduced downtime, and less management effort are benefits that speak for themselves.


Disadvantages
• Requires a constant internet connections
• Doesn't not work well in low speed connections
• May be slow
• Limited features

VI. ACKNOWLEDGEMENT

I am very thankful to my guide **mr.sachinsingh** for her support to write this paper. It is not a simple formal acknowledgement; it is note for thanks and regard to my side. Without your guidance and co-operation this paper will not conduct properly. I am grateful to my guide and my friends which helped me to take this paper at current level.

VII. CONCLUSION & FUTURE WORK

Cloud computing is a modern technology that can be used at large amount all over the world. If once a organization is decided to move with the cloud than it loose its control on the data. Amount of protection needed to secure data is directly proportional to value of data. Cloud security is depending on the trusted cryptography and computing. Now days, in educational and enterprises circle we use a large amount of cloud.

In this paper we discuss the security issues like authenticity, encryption, key management, trust and confidentiality and we explain the solution of those issues. Issues which is explain above are all the research hotspot of cloud computing, so cloud computing has bright future.

REFERENCES

[1] ***CLOUD COMPUTING SECURITY ISSUES &***RESEARCH ***CHALLENGES,RABI Prasad Pandhy, ManasRanjanPatra, International journal of computing science & information technology& security(IJCSITS) vol. 1, no.2, December 2011.***

[2] ***A REVIEW OF CLOUD COMPUTING SECURITY ISSUES,Manpreetkaur, Hardeep Singh International journal of advances in engineering & technology, June, 2015.***

[3] ***SECURITY ISSUES IN CLOUD COMPUTING-A REVIEW ,Irfan Hussain, Imran Ashraf International journal advanced networking & application.***

[4] *CLOUD COMPUTING SECURITY ISSUESIN-INFRASTRUCTURE AS A SERVICE,Pankaj Arora, RubalchaudharyWadhawana, International journal of advances research in computing science & software engineering, volume 2, Issues January 2012.*

[5] *ON TECHNICAL SECURITY ISSUES IN CLOUD COMPUTING,Meiko Jensen, JorgSchwenk, Nils Gruschkaj Luigi Lo Lacon o, 2009 IEEE International conference on cloud computing.*

[6] *REVIEW ON CLOUD COMPUTING SECURITY ISSUES AND ENCRYPTION TECHNIQUES,Jarpreet Singh, Sugandha Sharma, International journal of engineering development and research, volume 3.*

[7] *X. Zhang, N. Wuwong, H. Li, and X. J. Zhang, "Information Security Risk Management Framework for the Cloud Computing Environments", In Proceedings of 10th IEEE International Conference on Computer and InformationTechnology, pp. 1328-1334, 2010.*

[8] *R. L Grossman, "The Case for Cloud Computing," IT Professional, vol. 11(2).*

[9] *AmanBakshi, Yogesh B. Dujodwala, "Securing cloud fromDDoS Attacks using Intrusion Detection System in Virtual Machine," ICCSN '10 Proceeding of the 2010 Second International Conference on Communication Software and networks, pp. 260-264, 2010, IEEE Computer Society, USA, 2010. ISBN: 978-0-7695-3961-4.*

[10] *X. Harold C. Lin, ShivnathBabu, Jeffrey S. Chase, Parekh, "Automated Control in Cloud Computing:*

[11] *ISSN: 2249-9555.*