Internet & Web System
Term Paper
Dharti Patel – 02007206
Dharti_patel1@student.uml.edu

Cloud Computing

Abstract:

Cloud computing is a rapid evolving and promising technology. It allows you to access and store data over the Internet instead of your personal hard drive. Google Drive, iCloud, and Dropbox etc. This all are the cloud-based services that store all your data exclusively over the internet, freeing up storage space on your device. It is a product that combines different computing like grid computing, distributed computing, parallel computing, and ubiquitous computing. It uses a range of relatively advanced delivery models such as IaaS (Infrastructure as a Service***),*** SaaS (Software as a Service), PaaS (Platform as a Service) to deliver powerful computing capabilities. It aims to build and predict advanced service environments with a Service, using HaaS (Hardware as a Service) to distribute powerful computing power to end users. This paper describes the background and service models and discusses existing research issues and implications in cloud computing, such as security, trust, and privacy.

Introduction:

The future paradigm for computation has been predicted to be cloud computing. Applications and resources are both made available online as services in the cloud computing environment. The term "cloud" refers to an environment made up of hardware and software resources in data centers that offer a variety of services across a network or the Internet to meet user needs.[1]

According to the National Institute of Standards and Technology (NIST) [2], "cloud computing" refers to a shared pool of reconfigurable computing resources (such as networks, servers, storage, applications, and services) that require little management effort or communication with service providers and may be easily created and released. According to the justification, cloud computing provides simple, on-demand network access to a collection of pooled, programmable computing resources. Resources include things like software, virtual servers, platforms, network assets, computing infrastructure, and software services.

Cloud computing will make it simple to use services on demand. On-demand self-service, ubiquitous network connectivity, location-independent resource pooling, quick resource elasticity, usage-based pricing, and risk transference are some of the traits of cloud computing. The corporate and academic research sectors have paid close attention to these advantages of cloud computing. The world of business is currently changing due to cloud computing technology.

Cloud Architecture:

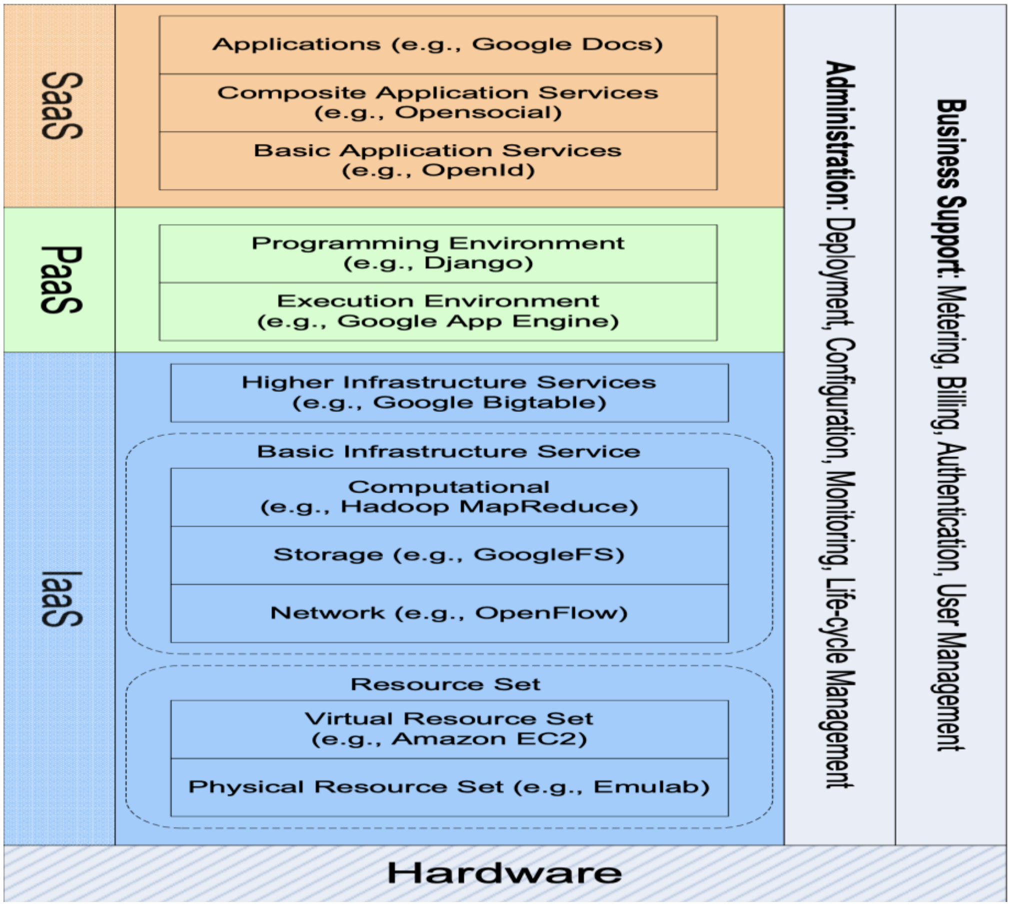
SaaS
Applications (e.g., Google Docs)
Composite Application Services (e.g., Opensocial)
Basic Application Services (e.g., OpenId)
PaaS
Programming Environment (e.g., Django)
Execution Environment (e.g., Google App Engine)
IaaS
Higher Infrastructure Services (e.g., Google Bigtable)
Basic Infrastructure Service
Computational (e.g., Hadoop MapReduce)
Storage (e.g., GoogleFS)
Network (e.g., OpenFlow)
Resource Set
Virtual Resource Set (e.g., Amazon EC2)
Physical Resource Set (e.g., Emulab)
Administration: Deployment, Configuration, Monitoring, Life-cycle Management
Business Support: Metering, Billing, Authentication, User Management
Hardware

Figure 1. Cloud Architecture

The general design of a cloud platform, also known as a cloud stack, is shown in Fig. 1. Cloud services may be provided in a variety of ways, from the bottom layer to the top layer, based on physical infrastructure (often backed by contemporary data centers). In the lowest layer, where resources are gathered and managed physically (e.g., Emulab) or digitally (e.g., Amazon EC2), infrastructure-as-a-service (IaaS) is provided. Services are provided in the form of storage (e.g., GoogleFS), network (e.g., Openflow), or processing capability (e.g., Hadoop MapReduce). Platform-as-a-Service (PaaS), which is offered by the middle layer, is an environment for programming (such as Django) or software execution (e.g., Google App Engine). Software as a Service (SaaS) is located on the top layer, where a cloud provider simply provides software applications as a service to further confine client flexibility. In addition to supplying services, the cloud provider also maintains a few management tools and resources (for instance, service instance life-cycle management, metering and billing, and dynamic configuration) to control a big cloud system.

Security in cloud Computing:

Owners are unable to monitor data in the cloud on the platform that can be used. For instance, the owner is unaware of the mission's execution status and the security of the data. To enable businesses and organizations to use cloud computing technology and provide their own data to CSPs (cloud service providers), it is crucial to investigate and resolve privacy and protection, encryption, access control, and trust issues. The stability of cloud computing is currently the most important topic under discussion. Data is at high risk if computer activities and transfers do not have sufficient security measures. Because cloud storage provides the possibility for a community of users to access the stored data, there is a likelihood of significant data risk. The finest security precautions must be followed by identifying security threats and solutions to these problems.

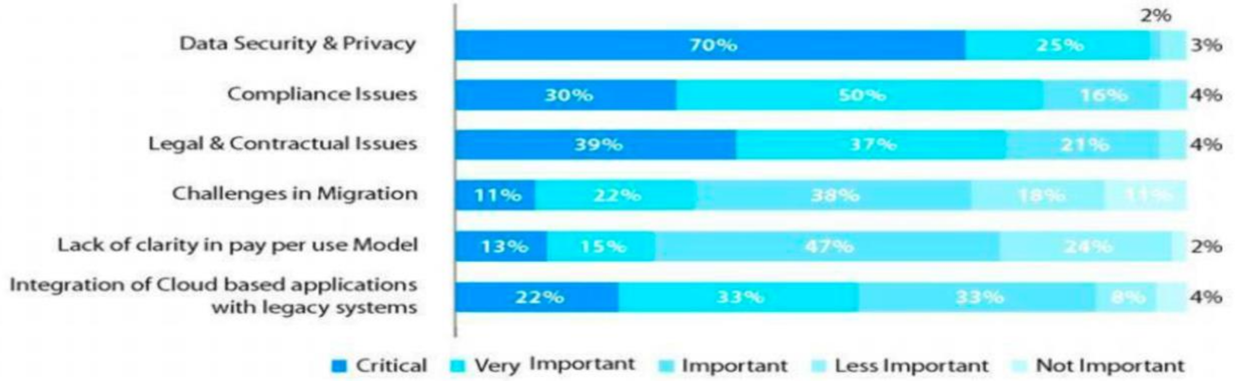

Figure 2

Figure 2 makes it clear that how data protection and privacy are considered is the most crucial and important factor to consider.

Data Security and Privacy:

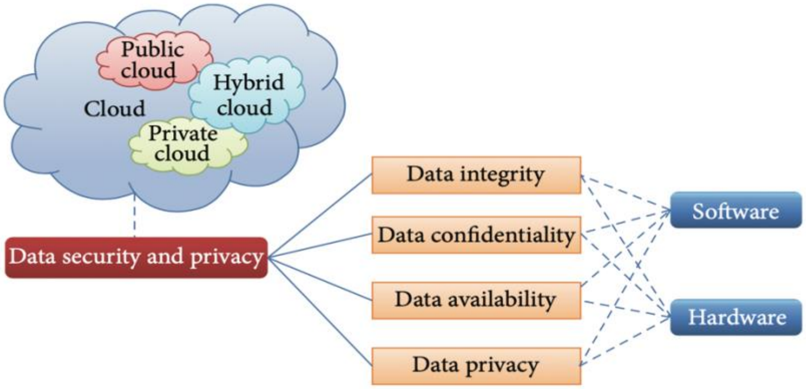

Figure 3

1)Data Integrity:

In a cloud system, maintaining data integrity involves protecting information integrity. Unauthorized users shouldn't lose the data or alter it. The foundation for offering cloud computing services like SaaS, PaaS, and IaaS is data integrity. In addition to large-scale data storage, cloud computing environments typically offer data processing services. Techniques like digital signatures and RAID-type schemes can be used to ensure data integrity.

In a cloud context, where there are many different entities and access points, permission is essential to ensuring that only authorized parties can interact with data. Organizations can boost their confidence in the integrity of their data by preventing illegal access. Greater insight into identifying who or what might have changed data or system information, potentially altering its integrity, is provided by the monitoring systems. It is expected of cloud computing companies to uphold data accuracy and integrity. However, in addition to consumers and cloud service providers, a third-party supervision system must be developed.

2)Data Confidentiality

Data confidentiality is essential if consumers are to store their private or confidential information on the cloud. To guarantee data confidentiality, authentication and access control mechanisms are employed. By improving cloud reliability and trustworthiness, the difficulties with data confidentiality, authentication, and access control may be resolved.

Users should avoid directly storing their sensitive data in cloud storage since users do not trust cloud providers and internal threats are nearly impossible to eradicate for cloud storage service providers. Simple encryption cannot fulfill complicated requirements like inquiry, concurrent modification, and fine-grained authorization due to the key management issue.

3)Data Availability

Data availability refers to how much a user's data can be used or recovered in the event of an accident, such as hard disk damage, an IDC fire, or a network failure, as well as how the user can independently verify their data rather than relying solely on the cloud service provider's credit guarantee. The issue of storing data on transborder servers is a serious concern for clients because cloud vendors are subject to local regulations and cloud customers should be aware of such restrictions. The cloud service provider must also provide data security, including data integrity and confidentiality. The cloud service provider should discuss all these worries with the client and establish a rapport based on trust. The cloud vendor should give clients assurances on the security of their data and explain to them the application of local laws. The study primarily focuses on data difficulties and challenges related to cost, availability, and security, as well as the location and relocation of data storage.

4)Data Privacy

Cloud computing's use of data privacy makes it possible to collect, store, move, and share data over the internet without endangering the privacy of individual users' personal information. Customers frequently are unaware of how the processing of their cloud-stored personal data takes place. With the popularity of the cloud growing, data privacy is turning into a crucial aspect of cloud computing. Millions of people are keeping their personal, professional, or both forms of data online as a result of the cloud's expanding popularity. Many cloud users aren't even aware of where the servers storing their data are physically located, much less how that data is being processed there. PII is at the heart of the concept of data privacy (Personally Identifiable Information). Utilizing personal data makes it simpler to find or identify a particular person. When combined with data from other sources, this information can also be used to identify a person.

Security Issues in Cloud Computing:

There is no denying that cloud computing offers a number of benefits, but there are also some security concerns. These Security Issues in Cloud Computing are listed below.

Data Loss: Data loss is one of the issues of cloud computing. This is often referred to as a data leak. We are aware that our database is not entirely under our control and that someone else has access to some of our sensitive data. Therefore, it is feasible that hackers will access our sensitive data or personal files if the security of a cloud service is breached.

Hackers' interference and unreliable API: As far as we are aware, if we are discussing the cloud and its services, we are also discussing the Internet. Additionally, we are aware that using API is the simplest way to interface with the cloud. Therefore, it is crucial to protect the APIs and interfaces that external users use. However, there aren't many services accessible to the public in cloud computing either. The vulnerability of cloud computing lies in the possibility that other parties could access these services. Therefore, it's likely that hackers could simply harm or hack our data using these services.

User Account Hijacking: The most important security problem with cloud computing is account hijacking. if a hacker manages to take control of a user's or an organization's account. The hacker is then completely free to engage in Unauthorized Activities.

Changing Service Provider: Another significant security concern with cloud computing is vendor lock-in. Changing vendors will present a variety of challenges for many enterprises. For instance, if a company wants to switch from Amazon Web Services (AWS) to Google Cloud Services, they will encounter a number of issues, such as the need to transfer all of their data, as well as issues related to the fact that the two cloud services utilize various different techniques and functions. Additionally, it's probable that AWS costs are different from those of Google Cloud and other services.

Denial of Service (DoS) attack: An excessive amount of traffic on the system can lead to this kind of attack. Large companies like those in the banking industry, the government sector, etc. are the primary targets of DoS assaults. Data loss occurs during a DoS attack. Therefore, it costs a lot of money and takes a lot of time to handle data recovery.

Conclusion:

The primary objective of this research was to examine and evaluate cloud computing security strategies for data protection. The newest and most promising technology for the next wave of IT applications is cloud computing. Data security and privacy concerns are a roadblock to the cloud computing industry's rapid expansion. Any firm must reduce the cost of data processing and storage, but analysis of data and information is always the most crucial activity for decision-making across all enterprises. To foster confidence between customers and cloud service providers, this study surveyed several data security and privacy information, with an emphasis on how data is stored and used in the cloud.

References:

[1] N. Leavitt, “Is cloud computing really ready for prime time?” *Computer*, vol. 42, no. 1, pp. 15–25, 2009.

[2] P.MellandT.Grance,“Thenistdefinitionofcloudcomputing,” *National Institute of Standards and Technology*, vol. 53, no. 6, article 50, 2009.

[3]https://www.researchgate.net/publication/260671144_Security_and_Privacy_in_Cloud_Computing

[4] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3879599

[5] https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-of-cloud-computing.html#:~:text=Cloud%20computing%20offers%20modern%20businesses,and%20more%20accessible%20than%20ever.

[6] https://www.iventuresolutions.com/blog/what-is-cloud-technology-how-does-it-work/#:~:text=In%20more%20advanced%20terms