

A Survey on Cloud Computing, It's Features and Its Security Challenges

Mithalee. V. Kadkol

Student, M.Tech 4th sem, CSE,
Sai Vidya Institute of Technology,
Bangalore, India
E-mail: mithaleekadkol@gmail.com

Mr. D. S. Harisha

Asst. Prof, Dept of ISE
Sai Vidya Institute of Technology,
Bangalore, India
Email: dsharirao@gmail.com

Sahana .P

Student, M.Tech, 4th sem, CSE
Sai Vidya Institute of Technology,
Bangalore, India
E-mail: sahanapandu22@gmail.com

Chaithrashree .B .A

Student, M.Tech, 4th sem, CSE
R N S Institute of Technology, Bangalore, India
Email: chaithrashree91@gmail.com

Abstract:- Cloud computing is an emerging technology that helps in providing a novel way with excellent facilities to perform computations. Cloud computing can also be known as a distributed computation since resources and applications platform are shared over the internet by means of on-demand service or pay-per-use due to the introduction of many cloud-based services and geographically diverse cloud service provides, sensitive information of multiple various entities are usually stored in remote servers. Due to this the security of the data stored in cloud has to be always high.

Keywords: cloud computing, security, pay-per-use, on-demand

I. INTRODUCTION

The Cloud Computing has come into the world of technology in the year 2000. Due to the unexpected and huge amount of success in utilization of the internet, there is an ubiquitous amount of computing resources that is available. Thus the cloud computing concept was realized or developed. Cloud computing is an emerging technology that provides IT services and resources to the client/customer by using internet.

Cloud Computing can be defined as a set of services that are enabled by the network by providing QoS –oriented, personalized, scalable, inexpensive computing platforms, depending on the demands, that can be accessed in an easy manner.^[1]

Some of the technologies that are utilized in cloud computing are Virtualization, Grid Computing and Utility computing. It also involves the Mainframe Computer, Peer-to-Peer type of Architecture.

- **Virtualization:** Virtualization software is essentially used to separate a physical computing device into one or more "virtual" devices. Each of these virtual devices can be easily used and managed to perform certain computing tasks. By using the operating system-level virtualization, we essentially create a scalable system of multiple independent computing devices. The computing resources that are idle can be allocated and used efficiently. This provides the strength that is needed to speed up IT operations, and reduce the cost due to increase in the infrastructure utilization

- **Grid Computing:** A form of distributed and parallel computing, where a 'super and virtual computer' consists of a group of networked, loosely coupled computers operating in tandem to perform very large tasks.
- **Utility Computing:** The packaging of computing resources, such as computation and storage, as a metered service similar to a traditional public utility, such as electricity.[2][3]
- **Main Frame Computing:** These are critically important computers that are used for doing critically important tasks, by large organizations.
- **Peer-to-Peer:** This type of architecture involves a distributed architecture rather than a centralized architecture.

The cloud computing has some attractive features that makes people depend on it and utilize it effectively as and when needed. The features are listed below.

- **Low Initial Investment:** The initial investment to set up a cloud and maintain it is less for a small organization as the maintenance is done by the cloud service provider as part of the SLA's.
- **Easy to Manage:** Since the management is done by the service provider, the cloud is easy to manage at the place of installation. Cloud computing helps users to use the application without installation and also allows access of personal files at any computer with the help of internet.
- **Scalable:** Cloud can perform equally well if the number of hosts connected to them, is increased or

decreased at any point of time. The performance is not affected.

- Ability to be deployed faster: Cloud is only to be installed at the client's computers. Due to this, the hardware and other infrastructure is not necessarily placed at the client's place. Hence it can be deployed faster.
- Independent of both device and location: Cloud is not affected by the place where its installed or the type of device it is connected to. It only need an internet connection to run smoothly.
- Reliable: The use of multiple redundant sites, makes cloud computing well-designed and suitable for businesses in business continuity and disaster recovery
- Secure: Cloud is secure as only the client's computers are connected to it. The data is always secure and ready to use.

Some of the other features are

- Confidentiality
- Integrity
- Availability

II. CLOUD CHARACTERISTICS

The National Institute of Standards and Technology defines the following five important characteristics that a cloud consists

- On-demand self-service: A cloud service user can one-sidedly provision the computational strength like the server time, network etc., without needing any human interaction for the same for each service provider.
- Broad network access: The access of the internet through the available broad bandwidth irrespective of the type of the client's platform is commendable.
- Resource pooling: The service provider's computational resources is pooled so as to serve many customer's using a multi-tenant model with varied physical and virtual resources to dynamically assign and reassign according to consumers demand.
- Rapid elasticity. Capacities can be elastically provisioned and released, sometimes automatically, to compensate for the demand. For the consumer, the capabilities that are available for provisioning often appear unlimited and can be assumed in any quantity at any time.
- Measured service. Cloud systems control and optimize resource automatically by leveraging a metering capability at some level of abstraction appropriate to the type of service. Resource usages can be monitored, controlled, and reported, thus providing transparency for both the service provider and consumer of the service.^[4]

Some other characteristics of cloud are listed as follows

- Agility
- Cost
- Multi-tenancy
- Performance
- Productivity
- Security

III. CLOUD SERVICE MODELS

Cloud Service Model is basically a type of model that the service provider provides depending on the type of services that are requested by the consumer. The three basic service models are

- Infrastructure as a service (IaaS): This type involves the virtual machines, servers, storage, load balancers, network etc.
- Platform as a service (PaaS): Cloud service providers deliver a computing platform, which typically includes operating system, programming language, database, execution environment, and web server. Application developers can develop and run their own software solutions on a cloud platform without involving the cost and complexity of buying and managing the underlying hardware and software layers.
- Software as a service (SaaS): Users are allowed access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is referred to as "on-demand software" as it is usually priced on a pay-per-use basis or using a subscription fee.

Some other types described by David Linthicum are Storage-as-a-service, Database-as-a-service, information-as-a-service, Application-as-a-service, Information-as-a-service.^[5]

Due to the above mentioned features, cloud is utilized so extensively in the current scenario of the IT industry.

The advantages of Cloud are

- Maintenance cost of hardware is less: This is due to the fact that the hardware is maintained by the cloud service provider
- Ease of access: The ease of access is possible since the cloud services can be accessed anywhere from the world, at any time if it is connected to the internet.^[6]

Some methods in analysing the security framework in cloud are

- Audit and Compliance: addresses data collection, analysing and archiving of data and prepared reports.
- Access control : this is done by Authentication
- Flow Control : Flow Control is mainly through exchanging data security and also by lifecycle of data security

- Identity and Credential Management: Identity is provided by the provider and credential involves user credentials like username, password etc..
- Solution Integrity: Cloud Service Provider provides a reliable, correct or credible operation by incident response and remediation, Fault Tolerance and Failure Recovery^[7].

The next section deals with the security issues involved in Cloud.

IV. SECURITY ISSUES IN CLOUD

Cloud computing is defined as a set of services that are enabled by the network by providing a scalable, Quality of Service, personalized, inexpensive computing platforms depending on the demands, which could be accessed in an easy manner by the consumer. Cloud offers systems/components as a service.

Cloud computing is divided into two parts user and cloud. User connects to a cloud through an internet.

Security is the top most challenge that is present in cloud computing, as there is huge amount of data/information that is stored in it and thus providing security to each and every data that is used by different client is difficult.

At some point of time, the processing has to be manually uploaded by a person to be included a cloud. At such situations certain concerns arise. They are

- Transmission of personal and sensitive data onto the cloud.
- Transmission of data from a remote cloud server to a client's computer.
- Storage of client's sensitive and personal information on a remote server that may not be owned by the client.^[8]

The last point is emphasized due to the fact that the cloud is a pay-per-use type of model. Due to this, there is a possibility that any unwanted user can sneak into any private computer by using different hacking methods. This leads to scope of accessing somebody's private and confidential data thereby raising security concerns.

Sometimes the authentication process is done in the cloud itself. This requires the cloud service provider or the service provider to outsource the authentication and other managerial aspects to a third party specialists in collaboration between themselves, by doing so, the performance and security issue to the cloud is passed as a message between third party and cloud service provider.

The above entire process is transparent to cloud users. The only goal of adding the above entire process is to increase the security in cloud.

Here, some other critical factors come into view. They are data location (remote location of data), location

transparency (as without gaining any knowledge about location, security facilities and features cannot be suitably added) and trust (the most important factor that need to be present on both CSP and third party authentication specialists). Thus AA can be used to build up trust on the providers of services.

Another way to provide security is to provide abstraction at different levels and also through scalability.

Even after performing additional tasks there is a possibility that some drawbacks arise due to the Cloud itself. Some drawbacks are

- Image filtering is not accurate when trying to upload on cloud. There can be discrepancies that can arise when a consumer may want to upload an image. The uploaded and the downloaded versions may vary slightly.
- Transport Cloud Protection System (TCPS) is a middleware whose main reason is to detect attacks as its present in between kernel and visualization layer. But it can't be implemented everywhere.

A. Concerns involved in Cloud

- Virtualization: Virtualization can be done at either operating system level or the Application level. It can be also present in either Server, Storage or at Network level. This leads to concerns regarding the confusion of the type of Virtualization used
- Network Security: Network Security involves the security of the network and the channel through which the cloud is connected to the consumer. If the network itself is not secure, there is changes of data being misused.
- Policy and Compliance: This refers to the policies and standards that the cloud service provider has agreed to provide to the consumer based on the price and type of use. The Compliance refers to adhering to these standards at all times without any interruptions by providing alternate methods if the service provider is currently unable to provide services.
- Data Location for data integrity: Maintaining the location of the data as confidential along with maintaining the data also to be confidential is important. Else the hackers after gaining knowledge on location of data can tamper with the data, resulting in integrity loss of data.

B. Security issues involved in Cloud

- Infrastructure Security
- Data Security and Storage
- Identity and Access Management
- Managing security
- Privacy^[9]

C. Schemes to improve Security

Since maintaining the security of the data is very important, certain schemes listed below can be used to help improve Security to some extent.

- Encryption scheme: By utilizing certain suitable encryption methods at different levels needed, the security of the data can be improved.
- Service providers have limited security: The cloud service providers must have limited or no access to the data. Only personnel at higher levels must be given authority to access data stored in their cloud.
- Stringent access controls for preventing unauthorized and illegal access by using Authentication, Authorization methods.
- Data back up and redundancy: Maintaining backup of the data and redundant data is very important. This can be used if any calamity occurs and the entire data present at a single location is lost.
- Data Integrity: Maintaining the integrity of the data by implementing abstraction of the data whenever and wherever required.

REFERENCES

- [1] Security issues with possible Solutions in Cloud Computing – A surey. Abhinay B. Angadi, Akshata B. Angadi, Karuna c. Gull . IJAR CET Vol 2, Issue 2, Feb 2013
- [2] It's probable that you've misunderstood 'Cloud Computing' until now". TechPluto. Retrieved 2010-09-14.
- [3] Danielson, Krissi (2008-03-26). "Distinguishing Cloud Computing from Utility Computing". Ebizq.net. Retrieved 2010-08-22.
- [4] "The NIST Definition of Cloud Computing". National Institute of Standards and Technology. Retrieved 24 July 2011.
- [5] An Advanced Survey on Cloud Computing and State-of-the-art Research Issues. IJCSI vol 9, issue 1, NO 1, JAN 2012
- [6] A Survey on Security Issues and Vulnerabilities on Cloud Computing. K.L.Neela Dept, of CSE, UVCE, Thirukkuvilai, Tamil Nadu and Dr. V. Kavitha, Dept, of CSE, UVCE, Nagercoil, Tamil Nadu(IJCSET)
- [7] Survey of Security Issues in Cloud Computing . Uttam Thakore, College of Engineering, University of Florida
- [8] Cloud Computing and Security Issues in the Cloud – Monjour Ahmed and Mohammad Ashraf Hossain. IJGDC Vol . 6, No.6(2013), pp 37-50
- [9] Survey on Cloud Computing Security. Shilpashree Srinivasamurthy, David . Q.Liu- Dept. Of CSE, Indiana University – Purdue University fort, Wayne.