IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Cloud Computing

Dr K.R.Khandait
Designation - Assist.Prof.
Name of College - Ajeenkya D.Y.Patil University
Pune, India
Names – 1. Aditya Raut, 2. Neha Shinde
Name of College - Ajeenkya D.Y. Patil University

***Abstract*: Cloud computing has emerged as a transformative paradigm in the field of information technology, offering on-demand access to a shared pool of configurable computing resources. This research conducts a comprehensive review of existing literature to investigate the current state of resource allocation strategies in cloud computing environments. The focus is on optimizing resource utilization, minimizing costs, and enhancing overall system performance.**

Keywords—Cloud computing, Systematic Mapping Study, Stacks, Tools, and Services

I. Introduction of Cloud Computing

Cloud computing is presently playing a significant role in the provisioning of vital services in information technology. A unique aspect of cloud computing is the cloud middleware and other related entities which supports applications and networks. Determining a particular research area especially in terms of cloud middleware and services at all levels could be a cumbersome process for a researcher, hence the need for reviews and paper surveys that identify research gaps. The purpose of this paper was to conduct a systematic mapping study of cloud computing middleware, stacks, tools and services at all layers. The focus was on three facets of studies, the research facet, topic facet and contribution facet.

A. HYBRID CLOUD COMPUTING

Hybrid cloud is a composition of a public cloud and a private environment, such as a private cloud or on-premises resources, that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources. It defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers. A hybrid cloud service crosses isolation and provider boundaries so that it cannot be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service. This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.

Another example of hybrid cloud is one where IT organizations use public cloud computing resources to meet temporary capacity needs that can't be met by the private cloud. This capability enables hybrid clouds to employ cloud bursting for scaling across clouds. It is an application deployment model in which an application runs in a private cloud or datacenter and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization pays for extra compute resources only when they are needed. Cloud bursting enables datacenters to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.

B. PRIVATE CLOUD COMPUTING

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third party, and hosted either internally or externally.[4] Undertaking a private cloud project requires significant engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. It can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management, essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".

C. *PUBLIC CLOUD COMPUTING*

Cloud services are considered "public" when they are delivered over the public Internet, and they may be offered as a paid subscription, or free of charge. Architecturally, there are few differences between public- and private-cloud services, but security concerns increase substantially when services (applications, storage, and other resources) are shared by multiple customers. Most public-cloud providers offer direct-connection services that allow customers to securely link their legacy data centres to their cloud-resident applications.

Several factors like the functionality of the solutions, cost, integrational and organizational aspects as well as safety & security are influencing the decision of enterprises and organizations to choose a public cloud or on-premises solution.

II. *THEORETICAL BACKGROUND*

The internationally agreed definition of cloud by the National Institute of Standards and Technology (NIST) is based on the cloud's requirements. The organization provides only an indirect definition and this definition does not include the goal of the cloud. The system without a goal looks like a system that only exists for its own sake.Therefore the definition should be made more applicable which contains the goal to be achieved. The cloud service has three actors: the customer, the vendor, and the legislator. Because of this, the definition is possible from more aspects. The purpose of the user who is the official customer of the service is other than the purpose of the vendor who is the manufacturer of the technology. Furthermore, the legislator has independent control. The different interests of the actors justify the conclusion of a service contract in which the parties should jointly formulate what they mean for services. The proliferation of cloud systems and the increasing number of disputes that are likely to appear require the definition of formal cloud service. Legislators can use this definition to statutory interpretation and dispute settlement. Furthermore, the robust cloud service providers are multinational companies nowadays who have taken into account disaster tolerance issues and have formed their systems in several countries or continents. So harmonization and internationally accepted interpretation are needed.

Definition of the cloud is possible from the following aspects:

- independent
- user
- contractual
- technological

A. INDEPENDENT ASPECT

From an independent perspective, the cloud definition, identification and classification types by NIST mentioned above can be the base in the legal systems of individual nations and the international alignment. According to this definition "cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction". This definition seems wordy and not exactly defined. This applies in general to an independent approach. The aspects of these definition types are to describe the behaviour of the system and the system is determined by its behaviour. From a special aspect, by contrast, the definition can have a more closed shape.

B. USER ASPECT

From the user approach, the cloud can be defined as such: the cloud is a combination of flexible computing services that can take over the interface of the service provider in order to implement more cost-effective business processes. The economic interests of the customer are dominant at this definition.The goal is the longtest cost-effectiveness [5]. It does not need a large IT operation to be maintained in case of recourse cloud services as a customer uses their infrastructure. Furthermore, the introduction of individual systems can be more flexible to manage.

C. CONTRACTUAL ASPECT

From the aspect of the customer and supplier cloud can be defined as the following: the cloud is a flexible information and communication technology service system that is made possible through an interface specified in the contract and agreed by both parties in quantity and quality. This definition is based on the parameters specified in the contract. This contract is an interface interpretation which is served between the supplier and the customer.

D. TECHNOLOGICAL ASPECT

From the topic relevant technological aspect, the cloud can be defined as the cloud is a flexible and measurable information and communication technology system in which the services behind the interface are as far as possible independent of the faults and limitations of physical and logical devices. This definition is based on the technology. Intrinsic properties of the cloud appear here which arise from the technologies used for building [5]. Before the introduction of technologies in order to increase transparency, one should discuss some of the basic concepts and requirements.

REQUIREMENTS

The analysis of cloud building technologies shows that the most important characteristics of the cloud include reliability, component variability, flexibility and the measurability of the services.

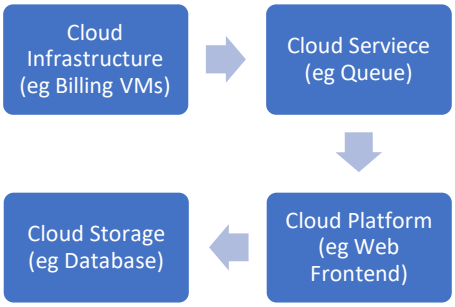
The technical requirements of the components can be grouped according to the following topics:

- availability (existence).
- virtualization of necessary resources (structural and energy knowledge).
- virtualization of implemented services (validation)

3. *RESULST AND DISCUSSION*

A. Cloud engineering

Cloud engineering is the application of engineering disciplines of cloud computing. It brings a systematic approach to the high-level concerns of commercialization, standardization and governance in conceiving, developing, operating and maintaining cloud computing systems. It is a multidisciplinary method encompassing contributions from diverse areas such as systems, software, web, performance, information technology engineering, security, platform, risk, and quality engineering.

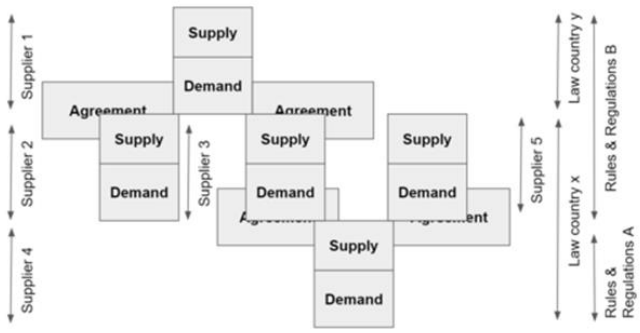


B. SECURITY AND PRIVACY

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end-users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access. Identity management systems can also provide practical solutions to privacy concerns in cloud computing. These systems distinguish between authorized and unauthorized users and determine the amount of data that is accessible to each entity. The systems work by creating and describing identities, recording activities, and getting rid of unused identities.

According to the Cloud Security Alliance, the top three threats in the cloud are Insecure Interfaces and APIs, Data Loss & Leakage, and Hardware Failure—which accounted for 29%, 25% and 10% of all cloud security outages respectively. Together, these form shared technology vulnerabilities. In a cloud provider platform being shared by different users, there may be a possibility that information belonging to different customers resides on the same data server. Additionally, Eugene Schultz, chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process he called "hyperjacking". Some examples of this include the Dropbox security breach, and iCloud 2014 leak. Dropbox had been breached in October 2014, having over 7 million of its users passwords stolen by hackers in an effort to get monetary value from it by Bitcoins (BTC). By having these passwords, they are able to read private data as well as have this data be indexed by search engines (making the information public).

There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership.[92] Physical control of the computer equipment (private cloud) is more secure than having the equipment off-site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services.[93] Some small businesses that do not have expertise in IT security could find that it is more secure for them to use a public cloud. There is the risk that end users do not understand the issues involved when signing on to a cloud service (persons sometimes do not read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is common and required for some services to work, for example for an intelligent personal assistant (Apple's Siri or Google Assistant). Fundamentally, private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.



. DESIGN OF CLOUD BASED SERVICE MODEL

Cloud-based design and manufacturing (CBDM) refers to a service-oriented networked product development model in which service consumers are able to configure products or services and reconfigure manufacturing systems through Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Hardware-as-a-Service (HaaS), and Software-as-a-Service (SaaS). Adapted from the original cloud computing paradigm and introduced into the realm of computer-aided product development, Cloud-Based Design and Manufacturing is gaining significant momentum and attention from both academia and industry. Cloud-based design and manufacturing includes two aspects: cloud-based design and cloud-based manufacturing. Another related concept is cloud manufacturing that is more general and popular. Cloud-Based Design (CBD) refers to a networked design model that leverages cloud computing, service-oriented architecture (SOA), Web 2.0 (e.g., social network sites), and semantic web technologies to support cloud-based engineering design services in distributed and collaborative environments. Cloud-Based Manufacturing (CBM) refers to a networked manufacturing model that exploits on-demand access to a shared collection of diversified and distributed manufacturing resources to form temporary, reconfigurable production lines which enhance efficiency, reduce product lifecycle costs, and allow for optimal resource allocation in response to variable-demand customer generated tasking. The enabling technologies for Cloud-Based Design and Manufacturing include cloud computing, Web 2.0, Internet of Things (IoT), and service-oriented architecture (SOA).

4. *CONCLUSION*

The goal of cloud computing is to allow users to take benefit from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs and helps the users focus on their core business instead of being impeded by IT obstacles. The main enabling technology for cloud computing is virtualization. Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With operating system–level virtualization essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations and reduces cost by increasing infrastructure utilization. Autonomic computing automates the process through which the user can provision resources on-demand. By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors.

5. *ACKNOWLEDGEMENT*

Cloud computing uses concepts from utility computing to provide metrics for the services used. Cloud computing attempts to address QoS (quality of service) and reliability problems of other grid computing models.

6. *REFERENCES*

- "Cloud Computing: Concepts, Technology & Architecture" by Thomas Erl:
- This book provides a comprehensive introduction to cloud computing concepts, technologies, and architectures. Thomas Erl is a recognized expert in the field.
- "Cloud Computing: Principles and Paradigms" edited by Rajkumar Buyya, James Broberg, and Andrzej M. Goscinski:
- This book is a collection of contributions from leading experts in the field. It covers various aspects of cloud computing, including architectures, applications, and security.
- "The NIST Definition of Cloud Computing" (NIST Special Publication 800-145):
- Published by the National Institute of Standards and Technology (NIST), this document provides a widely accepted definition of cloud computing and a comprehensive overview of its key characteristics, service models, and deployment models.
- "Cloud Computing: A Hands-On Approach" by Arshdeep Bahga and Vijay Madisetti:
- This book takes a practical, hands-on approach to understanding cloud computing. It covers various cloud platforms and services with examples and case studies.
- "Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide" by David S. Linthicum
- ACM Transactions on Cloud Computing (TOCC): The ACM Transactions on Cloud Computing is another respected journal that publishes research papers on cloud computing.
- David Linthicum is a well-known expert in cloud computing and service-oriented architecture (SOA). This book explores the convergence of cloud computing and SOA, offering practical insights for enterprises.
- "Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)" by Michael J. Kavis: This book focuses on design decisions for different cloud computing service models, providing valuable insights for architects and decision-makers.