Journal of Science and Technology

ISSN: 2456-5660 Volume 7, Issue 04 (JUNE 2022)

www.jst.org.in *DOI:https://doi.org/10.46243/jst.2022.v7.i04.pp88-98*

Addressing the Influential Factors of Cloud Computing: Assessment of Services under Deployment

Tanmaya Kumar Das[1], Sasmita Mishra, Ph.D,[2] , Hari Narayan Pratihari, Ph.D[3]

[1]*Ph.D Scholar, Dept. of CSE & Application, Indira Gandhi Institute of Technology, Odisha, India.*

[2]*Professor, Dept. of CSE & Application, Indira Gandhi Institute of Technology, Odisha,India.*

[3] *Professor, Dept. of Electronics & Communication Engineering, St. Martin's Engineering College, Dhulapally, Secunderabad, Telangana, India.*

[1]*research.tanmaya@gmail.com*

[2]*sasmita.mishra.csea@gmail.com*

[3]*drhnpratihari@gmail.com*

To Cite this Article

Tanmaya Kumar Das[1], Sasmita Mishra, Ph.D,[2] , Hari Narayan Pratihari, Ph.D[3]" **Addressing the Influential Factors of Cloud Computing: Assessment of Services under Deployment"**, *Journal of Science and Technology, Vol. 07, Issue 04, June 2022.*

Article Info

Received: 25-04-2022 *Revised: 11-05-2022* *Accepted: 02-06-2022* *Published: 27-06-2022*

Abstract: *As a new paradigm, cloud computing is drawing interest from organizations, communities, and individuals who believe it has the ability to revolutionize the way to do business. Traditional IT governance challenges are addressed while also providing possible benefits by this technology. If any business organization wants to remain competitive, it must keep up with technological advancements. Users have more alternatives when it comes to cloud computing because there are numerous service models and configurations. A multi-tenant system with a common pool of resources, and consumers from all walks of life, socio - economics, technology, geographic location and service requirements has always been a serious security issue. As a result of cloud computing deployment or management, as well as some other concerns like choosing the most appropriate cloud setup, real-time monitoring requirements and dependency on service providers and cloud management and data recovery are all hazards that can occur. Moreover, in a small percentage of cases, this can result in reality consequences. This paper focuses on cloud computing security, risk, and privacy concerns, along with other influencing factors.*

Keywords: *Cloud Computing, Cloud influencing Factors, Cloud Deployment, Cloud Security & Risks*

I. Introduction

Cloud computing has emerged as a formidable competitor in the realm of information technology. It is widely acknowledged as one of the most significant factors, not only in terms of data storage but also in terms of data protection, accessibility, and cost efficiency. As a result of advances in technology, not only has the number of people using the internet significantly increased, but so has the price of associated hardware and software. The concept of cloud computing has successfully gained a lot of popularity in a relatively short period of time in order to minimize the cost of hardware and software by supplying services when consumer demands are made via the internet. One of the key reasons for managements to move their focus toward IT is cloud computing, which is not a new concept but has recently become a paradigm of solutions. [1] Cloud computing is not a new concept but has lately become a paradigm of solutions. It is required of them to pay billings for only the resources that they actually use up. One of the most important technologies that make cloud computing possible is virtualization, which separates real computing systems into two or more virtual computing devices to make it easier to handle computing operations. Pay-as-you-go is the payment model that is utilized for cloud computing services. The availability of high-capacity networks, low-cost computers and gadgets, and broad use of hardware virtualization, Service-Oriented Architecture (SOA), Automatic, and Utility computing have all contributed to the rise in popularity of cloud computing. Cloud computing has recently become an extremely popular service due to the numerous benefits it offers, including high computational power, low service prices, scalability, high performance, and

accessibility [2]. However, before widespread commercial use can become a reality, considerable advancements are required in the areas of security, risk, and privacy.

II. Background and literature review

Because of rapid developments in processor and storage technology as well as the growing popularity of the Internet, computing resources have become more broadly available, more powerful, and more affordable than they have ever been before. This progression in technology has led to the development of a novel computing model known as cloud computing, in which resources (such as CPU and storage) are provided as general utilities that users can lease and release on-demand over the internet. The conventional function of service provider in a cloud computing environment is divided into two categories: infrastructure providers, who operate cloud platforms and lease resources based on demand, and service providers, who rent resources from one or more infrastructure providers in order to serve end users [2]. Large companies such as Google, Amazon, and Microsoft are competing to provide more powerful, reliable, and cost-effective cloud platforms, and businesses are looking to reshape their business models in order to take advantage of this new paradigm as a result of the advent of cloud computing over the past few years. [2].

The Cloud Deployment Models

The cloud deployment paradigm, which illustrates how people interact with resources and network infrastructure in diverse locations, is a key component of implementing a cloud system. The final determinant of the model's form and size is the cloud infrastructure's purpose and rate of availability. Only a few features can be used to distinguish between the fundamental models, like ownership, access control, and security protocols. Five alternative cloud computing deployment models have been implemented till date [16].

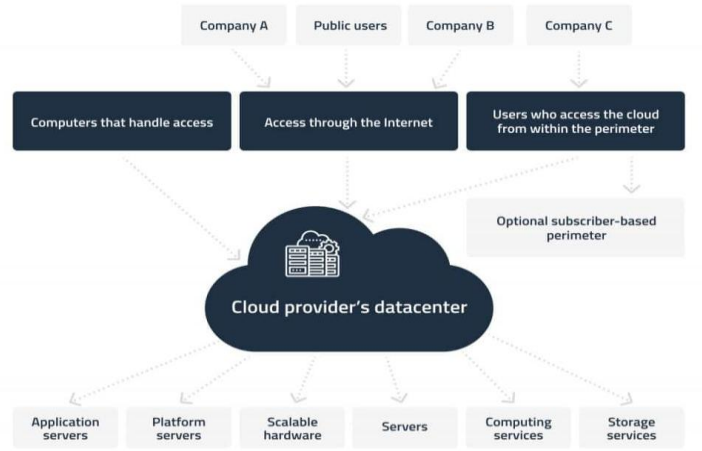

Fig.1: Public cloud

Public cloud: There are no limitations on the uses or methods of access for this type of cloud infrastructure, thus anyone can use it for anything at no cost. Examples of similar services include Amazon Elastic Compute Cloud (EC2), IBM Cloud, Google App Engine, Microsoft Azure, and others. Customers don't have to worry about buying and maintaining their own equipment when a service provider looks after the infrastructure. For the resources they receive as a service, clients pay providers on a pay-per-use basis. The entire transaction is completed out online. These resources can be increased by the user to meet their specific needs, makes it the ideal option for a variety of organizations in low-privacy sectors. [16].

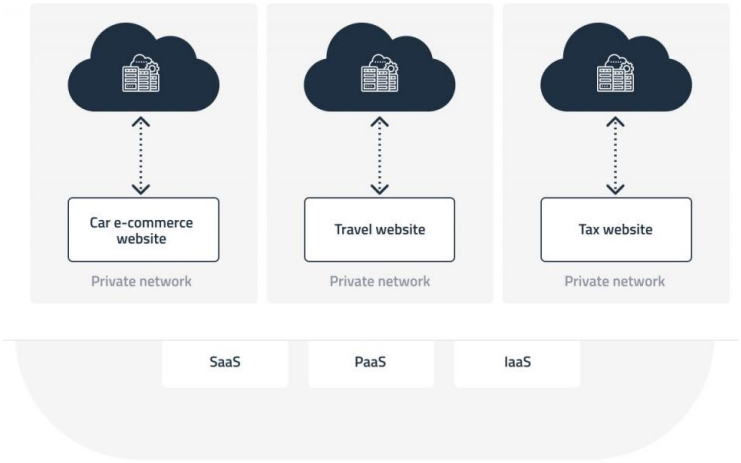

Fig.2: Private cloud

Private cloud: The underlying technology has not changed significantly from the public model. The use of a private cloud infrastructure by just one business characterizes this type of cloud computing. Only those who have been allowed access may use the system and services. The IT departments of the same business are in charge of maintaining and protecting the cloud, thus the security measures there are more stringent. This is a great option if any company is worried about data security [16].

Fig.3: Community cloud

Community cloud: This infrastructure can be used by specific user groups. Similar to the private deployment model, the server and its associated resources are owned by a number of firms that carry out comparable or comparable computational operations as opposed to just one organization. Banks, partnerships, and other similar entities are examples of this kind of organization [16].

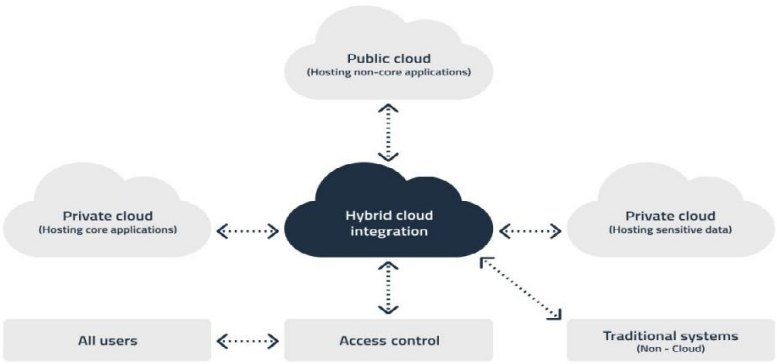

Fig.4: Hybrid cloud

Hybrid cloud: This particular cloud deployment technique enables the integration of cloud servers from several manufacturers into a single architecture while maintaining their individual identities. The public system can take care of ancillary duties like workload analysis for development and testing. The most economical and quickest solution currently available is to protect and preserve strategic assets in a hybrid cloud. Additionally, this architecture makes moving data and programs around the system much simpler and more effective [16].

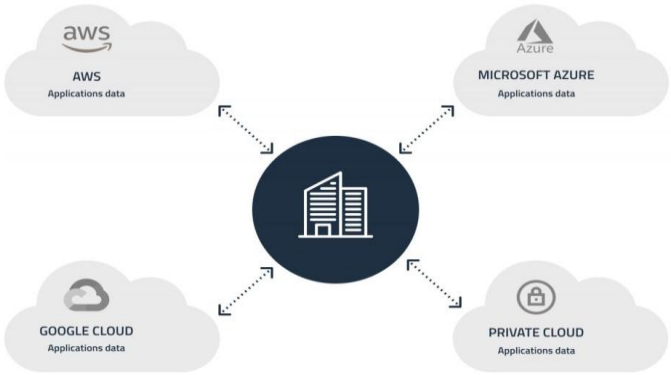

Fig.5: Multi cloud

Multi-cloud: In order to accomplish their goals, multifaceted deployment models mix the services of many cloud providers simultaneously. This is comparable to a hybrid architecture but enables the use of numerous public cloud services. This improves service availability when utilizing services from many clouds, which is beneficial for redundancy [16].

There are several applications for various cloud deployment models. For a variety of reasons, for instance, certain businesses are better suited for using public cloud services. They are not desired to be used by those who find them complicated, secret, or legally protected as intellectual property. The best models are chosen as a result of the user's requirements [16].].

- Convenience: Public, community, and multi-cloud systems are the best because the ISP does the majority of the work.
- Ease of use: the public cloud and multi-cloud architectures are the most user-friendly options in this regard; however, hybrid cloud architectures can also be used effectively with the appropriate configuration settings [16].When community members work together, the data control capabilities of private, hybrid, and public clouds are elevated to a higher level of sophistication [16].
- Reliability: The reliability of a private cloud is considered to be the highest available. If it is properly tuned, a hybrid instrument can have a level that is enough for the situation [16].
- Scalability: Private and hybrid cloud environments offer the highest capabilities in this regard. Private clouds, public clouds (provided that participants conform to the company security policy), and hybrid clouds are all considered to have a higher level of security and secrecy than public and private clouds[16].

- Flexibility: When it comes to flexibility, private and hybrid clouds are your best bet because no one disturbs you to settle your resources in either of those environments [16].
- Cost: Because the cost is shared across users, public and community clouds are the most cost-effective alternatives. They also offer the lowest costs overall [16].
- Hardware needs: By definition, public clouds and community clouds do not have any requirements in this area.In spite of the numerous cloud deployment models available, users still have the option of configuring and managing their hardware in accordance with one of several fundamental service models. These models include the following [16]:

IaaS is an abbreviation for "infrastructure as a service (IaaS). Users can access cloud resources, including computing, networks, and cloud storage, via a network connection provided by the service. IaaS data storage providers, like DropBox, have seen their customer base expand as a result of the proliferation of big data, mobile applications, and Internet of Things (IoT) networks [16]. A business model known as "platform as a service" (PaaS), where the users are given access to an application software platform, as well as all of the necessary information technology infrastructures, so that they can run the programme using a network connection [16]. The delivery of computer programmes to users on a subscription basis (SaaS). Through a connection to a network, it provides users with an application that is fully operational, in addition to the platform on which it operates and the information technology infrastructure that it requires. This is the standard method via which cloud applications are made available [16].

Benefits of Deploying Platforms in the Cloud

1. Cost savings: It is feasible to substitute costly investments in infrastructure, software licensing, technical employees, and so on with easy monthly payments instead. This can result in significant cost reductions. For instance, it has been projected that transitioning an organization's email to a solution hosted in the cloud can result in cost savings of approximately 30 percent for that organization. The relocation of the customer relationship management system to the cloud may also result in cost reductions of up to 25 percent. In spite of the fact that businesses could make mistakes that drive up prices, expenses can be kept to a minimum by careful planning and the solicitation of trustworthy counsel from a third party[16]. The business model of a cloud-based solution includes the ability to pay only for the resources that are really used, so lowering the initial threshold of substantial investment and allowing for the achievement of goals at a later date. The new model is significantly more suited to reflect the cash flow of business [16].
2. Scalability means that it can progress from solutions that are easier to understand to applications that are more difficult. Also, the auto-scaling features that are inherent in cloud solutions ensure that you will always have the correct capacity and performance at any given time. This prevents you from having to oversize your infrastructure in order to meet unexpected peak needs [16].
3. Accessibility and portability: It enables users to access services and information stored in cloud applications from any location in the world through the Internet, utilizing any fixed or mobile device that they choose [16].
4. Technology that is always up-to-date: The service provider is responsible for updating and improving the systems, which ensures that the company always has access to the most recent technology without the need to make significant investments in the Product Update/Upgrade planning, development, execution, and post-migration processes [16].
5. Reduced Effort and Resources Necessary to Manage ICT Systems: This feature enables the company to direct its attention toward the management of its business operations, thereby lowering the amount of effort and resources that are required to successfully manage its ICT systems [16].
6. Ease of Access: Access to any information, both in real time and in shared form, from any location and via any device — as long as it has an Internet connection [16].
7. Simple Handling: There is no need for any kind of intervention in the integration process. Because integration of systems happens nearly automatically in the cloud, businesses do not need to worry about resolving difficult technical interoperability issues. This frees them up to focus on other priorities. The integration of solutions within the cloud not only provides businesses with access to information that is consistent and integrated across all of the solutions, but it also removes the necessity for organizations to complete data registration chores in a redundant manner. Software is kept up to date in an automated manner, so users may always access the most recent version. Cloud computing solutions can be tailored to meet the specific requirements and demands of each individual customer [16].

Challenges of Deploying Platforms in the Cloud

1. Security: The most major obstacles include the loss of data, concerns regarding confidentiality, and security breaches. The successful rollout of an appropriate application will alleviate sufficient anxiety to allow for transfer to the cloud. Due to a lack of resources or previous experience, it can be difficult to recruit individuals who possess the requisite

abilities. Using an external provider that has previous experience managing cloud services could be one answer to the problem. Governance: Some firms do not have visibility into the shadow IT, and governance gets more challenging in hybrid cloud systems as well as many other cloud environments. The use of best practices, the implementation of policies, and the employment of a managed service are all ways in which procedures can be made more straightforward [16].

2. Compliance: When it comes to compliance management, having the abilities necessary to preserve the information, find solutions to problems, and give proper compliance reports is essential[16]. When it comes to migration, enabling a new application to run in the cloud is a relatively straightforward process; however to migrate an existing application to that environment presents a number of challenges. It is necessary to do pre-tests in order to be certain that a migration will be completed successfully and on schedule. The creation of a project timetable and the selection of a subject matter specialist are also additional aspects to take into consideration [16].Integration presents a difficulty in this context since it is necessary for services and applications running in the public cloud to be able to function in tandem with their counterparts running in the private cloud or on-premises systems [16].
3. Quality of Service: It is vital to develop a service level agreement (SLA) in order to assure server uptime, performance, and latency in the Internet connection; or the acquisition of systems, administration, and maintenance.

As a result, the cloud provides a means of maintaining one's competitive edge in the face of rapidly accelerating changes in business practices, technological advances, and economic conditions. Despite the difficulties, the benefits it delivers, which help to strengthen not only the technological infrastructure but also business processes, more than make up for it [16].

Businesses are increasingly resorting to hybrid multi-cloud setups in an effort to enhance team productivity, rapidly scale their IT infrastructure, protect their data, reduce operational costs, and ultimately create business value. Scale, speed, and convenience are all good things, but they also bring with them an increasing level of complexity. Complicated systems have a higher chance of causing harm than simpler ones [16].

Cloud service providers must therefore manage the risks associated with a cloud computing environment in order to identify, assess, and priorities the risks in order to reduce these risks, improve security, increase trust in cloud services, and alleviate organizations' concerns over the issue of using a cloud environment[16].

The purpose of this research is to address some of the most important issues of cloud computing, such as security, risk, and privacy. Several security issues arise because of the broad scope of cloud computing, which encompasses a wide range of technologies such as network architectures and databases as well as operating systems and virtualization techniques such as resource allocation and management. Thus, many of these systems and technologies have security flaws that affect cloud computing [2].

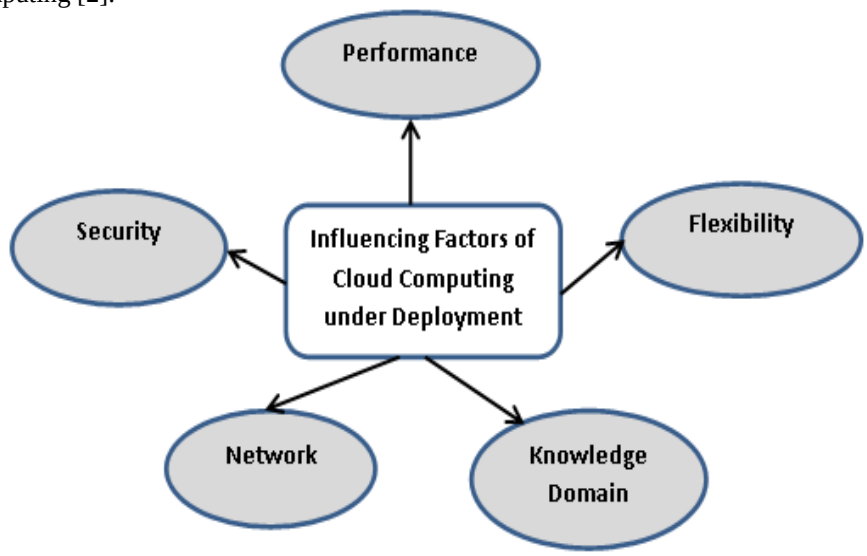

Fig.6: Influencing factors of cloud computing under deployment

Recent trend influential factors of cloud computing

Cloud computing has its advantages, but it also has its drawbacks. In some circumstances, this can lead to significant challenges. Cloud computing ghosts, such as the following, exist in the real world.

- Security issues: Many organizations are concerned about data security while migrating to the cloud. In most cases, the cloud service provider is responsible for ensuring the security of its clients' data because they all share one server. Data integrity is guaranteed by the cloud service provider, but businesses are still responsible for protecting their own data. Hacking and other security breaches are a typical issue.. Even if a company's data is accidentally or maliciously leaked, customers will lose trust in its products and services [7].
- Performance challenges: In today's highly environment, many businesses are looking for cloud computing to improve system performance. Because clients will migrate to another service provider if cloud performance isn't up to grade, this is a major concern for the organization. Web page and application loading times can have a significant impact on the amount of people who use them. Service providers' inefficient traffic splitting may be to responsible for the delay. It can be difficult to maintain operations even if one or more components fail in a fault-tolerance environment. [13].
- Network dependency: High-speed networks are required for cloud computing, because it entails a great amount of data being transported. With limited bandwidth, data transfer across the network may be problematic. In order to avoid commercial losses, organizations must invest more in high-speed networks, even if they may reduce the hardware expenses. Network bandwidth, which can be expensive, becomes an enormous burden for a small business organization. [14].
- Lack of knowledge: Due to its complexity, cloud computing demands more research and is a time-consuming task. This requires a substantial amount of knowledge and experience. Numerous professionals in the industry can perform this task; however it is typically a well-compensated vocation. This increases the cost of doing business for small business organizations even further. [11].
- Lack of flexibility: When an organization has been adopting cloud services from a certain provider for an extended period of time and wishes to transition to a different cloud-based service provider, it is typically a tough process that requires reengineering. There is a loss of flexibility when migrating from one cloud to another. [10].

III. Contribution

Deploymental research challenges

As a result of the widespread adoption of cloud computing, cloud computing research is in its infancy. On a regular basis, new problems arise in commercial applications that have not yet been addressed by researchers. In this part, while the projects are being implemented, we discuss some of the more difficult cloud computing research challenge [15].

- **RQ1. Automated service provisioning:** One of the most significant benefits of using cloud computing is the users having the ability to acquire and release resources at their convenience. In the context of this scenario, the objective of a service provider is to distribute and reallocate cloud resources in order to achieve its service level goals while simultaneously reducing its operational costs. On the other hand, it is not quite obvious how a service provider can achieve this objective. Finding out how to tie SLOs like Quality of Service (QoS) needs to low-level resource requirements like CPU and memory can be a particularly challenging task. In addition, choices regarding the provisioning of resources need to be made in a dynamic manner in order to achieve a high level of agility and respond to sudden shifts in demand. One example of this is when a large number of users use the same online service at the same time. The challenge of automatically providing services is not a recent development. [10]. The topic of dynamic resource provisioning for Internet applications has received a lot of attention in the past. These approaches typically entail:
  1. Constructing an application performance model that predicts the number of application instances required to handle demand at each level in order to meet QoS requirements and constructing an application performance model that predicts the number of application instances required to handle demand at each level in order to satisfy QoS requirements.
  2. Periodically predicting future demand and determining resource requirements using the performance model; and
  3. Automatically allocating resources using the predicted resource requirements.
- **RQ2. Virtual machine migration**: Virtualization can offer significant advantages in cloud computing since it makes it possible to move virtual machines from one data centre to another in order to distribute the load. The provisioning of a data centre can become more robust and responsive after virtual machine migration has been completed. Methods for migrating processes have developed into what is now known as migrating virtual machines. Both Xen and VMware have added support for "live" virtual machine (VM) migration, which entails extremely small periods of downtime ranging from tens of milliseconds to one second. When moving an entire operating system along with all of its

applications as a single unit, it is possible to sidestep many of the issues that are presented by migration approaches that operate at the process level. The elimination of hotspots is the primary advantage of virtual machine migration; yet, doing this operation is not a simple endeavor. The ability to quickly adjust to sudden shifts in workload is currently lacking in both the process of detecting hotspots in the workload and beginning a migration. In addition to this, the state of the memory should be conveyed in a consistent and efficient manner, taking into consideration the resources of the application as well as the physical server. [4].

- **RQ3. Server consolidation:** Increasing resource utilization while simultaneously reducing energy consumption is possible with server consolidation, which is an important factor in the world of the cloud. In many cases, the technology known as "live VM migration" is used to consolidate virtual machines (VMs) running on several underutilized servers onto one single server, allowing the remaining servers to be powered down. A number of heuristics have been developed, and in recent years, the interdependencies between virtual machines (VMs), such as the need for communication, have been examined. Instead of slowing down apps, a consolidated server environment should actually improve them. Virtual machines (VMs) are well-known for consuming varying amounts of resources over the course of their lifetime. Maximizing server consolidation may cause resource congestion if a VM changes how much of the server's bandwidth, memory cache, or disc I/O it requires when its virtual machines (VMs) share those resources. Since virtual machine resource consumption can fluctuate, it's critical to monitor it and use the information collected to combine servers efficiently. When resources are stretched too thin, the system must be able to immediately adjust its response. [4].
- **RQ4. Data security:** In addition to cloud computing, data security is a major focus of research. Because service providers rarely have access to the physical security systems of data centers, they must rely on the infrastructure provider to offer total data security. Even with a virtual private cloud, the service provider has no way of confirming that the security parameters have been properly implemented.[8]. These objectives must be met by the infrastructure supplier in this case.
  1. *Confidentiality*, for secure data access and transfer, and
  2. *Auditability*, for attesting whether security setting of applications has been tampered or not.
  3. *Cryptographic protocols* are commonly used to establish confidentiality, whereas remote attestation techniques can be used to achieve auditability. As proof of system security, remote attestation normally requires a trusted platform module (TPM) to provide non-forgeable system summary (i.e. system state encrypted using TPM's private key). In a virtualized system, such as the cloud, VMs might dynamically relocate from one location to another; therefore remote attestation alone is insufficient [4]. In this instance, trust mechanisms must be built at every architectural layer of the cloud. To begin, hardware TPM must be used to trust the hardware layer. Second, employing secure virtual machine monitors, the virtualization platform must be trusted. Only enable VM migration if both the source and destination servers are trustworthy [14].. Recent research has focused on developing effective trust establishment and management mechanisms.
- **RQ5. Software frameworks**: Hosting large-scale, data-intensive applications on the cloud is a viable alternative. MapReduce frameworks like Hadoop [10] are commonly used for scalable and fault-tolerant data processing in these applications. MapReduce task performance and resource consumption can be significantly affected by the type of application being used. I/O costs are high for some Hadoop operations like sort, and CPU power is high for others like grep. Additionally, the virtual machine (VM) given to each Hadoop node may differ in some respects. When multiple virtual machines are housed on the same server, the bandwidth available to each one is limited [4]. As a result, it is possible to maximize the performance and cost of a MapReduce application by carefully picking configuration parameters and developing more effective scheduling algorithms. Removing bottleneck resources can significantly improve application execution time. Hadoop operations (online or offline) and adaptive scheduling in dynamic conditions are two of the most difficult problems to model and solve. There is often a trade-off between energy awareness and performance as well. A study subject that has still to be investigated is how to find a good trade-off point based on the purpose. [11].
- **RQ6. Storage technologies and data management:** There are software frameworks, such as MapReduce, developed for distributed processing of data-intensive activities such as Hadoop and Dryad. Google File System (GFS) and HDFS are two popular Internet-scale file systems that are often used by these frameworks. These file systems aren't like normal distributed file systems in terms of storage structure, access pattern, and application programming interface. As a result, compatibility issues arise with older file systems and software. [10].
- **RQ7. Data Centric Architectures:** Currently, the most of commercial clouds are deployed in huge data centers and run centrally, in accordance with the current trend. As much as this design saves money by using a larger footprint, it

also has drawbacks, such as higher energy expenses and a higher initial investment in the data centre. As a result of recent study, compact data centers may be a better option in many cases: they don't use as much power, so they don't need a sophisticated cooling system; they're less expensive to create and more widely distributed. Time-sensitive services, such as content distribution and interactive gaming, frequently call for geographic diversity [15].

A lack of control over software, platform, and/or infrastructure in the Cloud is a major security problem, according to numerous studies. Data will be virtualized and stored in the Cloud on a distributed network of computers. In the commercial sector, the cloud opens up a new channel via which a service or platform can be offered. As a result, the Cloud environment may face the greatest threat to security. Cloud clients will have no control over their own data and software, there will be no oversight of Cloud providers, and the data owner may not be aware of where data is physically located at any one time [13]. Cloud computing may be threatened by open-source Cloud infrastructure that is accessible to the general public, yet owned by corporations who provide Cloud services. In cloud computing, applications and data are generated and maintained by users and may only be accessed through a specific cloud's program, platform, or infrastructure.

Guidelines for managing issues

Cloud computing environments are multi-domain systems with variable security, privacy, and trust criteria for each domain, as well as diverse mechanisms, interfaces, and semantics. Individually enabled services or other infrastructure and application components could be represented in such a domain. A logical fit for service composition and orchestration is service-oriented architectures (SOA). Developing a comprehensive policy-based management framework in cloud computing environments is essential, using existing research on multi-domain policy integration and secure service composition. If cloud computing is to be extensively utilized, the following security and privacy issues must be solved. [15].

- **Authentication and identity management:** It is possible for people to share their personal information with a wide range of services on the Internet by utilizing cloud services. An identity management (IDM) strategy can be used to authenticate both users and services. Using distinct identity tokens and identity negotiation techniques is a big concern when it comes to cloud-based IDM. Password-based authentication has a built-in vulnerability and presents a severe security risk. In order to maintain the privacy and security of both users and processes, an IDM system is a need. Cloud computing in multi-tenant configurations, on the other hand, has the potential to damage identity information privacy in ways that are as yet unknown[6]. Protective measures may become more challenging if they must contend with multiple jurisdictions. Depending on the front-end service, it may be necessary to protect the user's identity from other services. Authentication and identification information must be kept separate in multi-tenant cloud systems. Integration with other security components should be as easy as possible. Authentication and identity management in the cloud must be designed and implemented thoroughly. [6].
- **Access control and accounting:** Because of the variety and complexity of cloud computing services, as well as the domains' differing access requirements, fine-grained access control policies are necessary. Access control services, in particular, must be able to capture dynamic, context, attribute, or credential-based access requirements while also enforcing the principle of least privilege. There may be a need for access control systems like these to incorporate privacy-protection requirements, which are typically represented as complex rules. It is imperative that the cloud access control system is easy to use and that permissions are distributed correctly. There must be a policy-neutral specification and enforcement mechanism for handling cross-domain access difficulties in order for cloud delivery models to have acceptable interoperability[4]. Thus, researchers need to implement a privacy-aware architecture for access control and accounting that is easily auditable as soon as possible.
- **Trust management and policy integration:** Multiple service providers cohabit in the cloud and collaborate to provide different services to users, but their security techniques and privacy procedures may differ. Therefore, we need to deal with the diversity of their approaches to policy-making. Cloud service providers may have to mix multiple services in order to supply larger applications. Security methods are needed to ensure that the dynamic collaboration is managed safely and that security breaches are successfully monitored during the interoperability process, as a result. When domain policies are checked individually, security violations can still occur during integration. Since policy integration can lead to security breaches, providers must be careful to manage access control policies[16].

  In cloud computing, interactions between different service domains might be dynamic, transient, and intensive according to service requirements. Cloud computing The design of a trust framework is therefore necessary to capture generic factors for building trust and to keep track of changing trust and interaction/sharing needs as they

change. Policy integration tasks in the cloud should also be able to deal with issues such semantic heterogeneity, secure interoperability, and policy evolution management. Consumer perception can shift at lightning speed, necessitating a trust-based, secure interoperability framework that can help establish, negotiate, and maintain trust. It's a well-known issue that wireless and peer-to-peer network trust management frameworks need to be improved. There is, however, a pressing need for cloud computing environments to have reliable and robust trust models. This will be a difficult problem to solve because of various interoperability issues and the global deployment of cloud service delivery models[16].

- **Secure service management:** Customers of cloud service providers and service integrators benefit from the creation of new services in the cloud. Customers' security requirements can be met through a framework provided by the service integrator, which enables independent service providers to coordinate and interwork services as well as collaborate to create new services[9]. Traditional Web Services Description Language (WSDL) does not adequately describe cloud computing services, even though many cloud service providers use it. SLAs, pricing, and quality of service (QoS) are all crucial aspects to keep in mind while evaluating cloud computing options. These difficulties must be addressed in order to characterize and introduce services, locate the best interoperable solutions, and integrate them without breaking the policies of the service owner and ensuring that SLAs are met. Furthermore, an automated and systematic service provisioning framework that takes into account security and privacy concerns is essential[8].
- **Privacy and data protection:** When it comes to cloud computing, many of the issues relate around privacy, including protecting personal information, integrating policies, and keeping track of transactions. In many cases, companies are wary about storing their data and applications on systems that aren't housed in their own data centers. In a shared infrastructure, customers' sensitive information is at increased danger of being accessed and exposed by others. Cloud service providers must reassure their clients and give a high level of transparency into their operations as well as privacy protection[6]. All cloud security solutions must have privacy-protection capabilities. In a similar spirit, it's becoming increasingly crucial to know who invented, who modified, and how. This information could be used to trace back, audit, and implement history-based access control. Managing data provenance and privacy in cloud systems where physical boundaries have been erased is a huge challenge. In addition, this is a significant scientific challenge[6].
- **Organizational security management:** Security management and information security lifecycle models are fundamentally altered when companies move to the cloud. Shared governance, in particular, can become a major problem if it isn't addressed correctly. Despite the potential advantages of cloud computing, it may lead to less cooperation across multiple communities of interest inside client enterprises. [5]. Concerns regarding responding to security issues quickly and developing systematic business continuity and disaster recovery strategies are also raised when relying on external companies. Third parties are also required for risk and cost-benefit analyses. For this reason, consumers must evaluate novel risks, such as data leaking in multi-tenant clouds, as well as resiliency issues, such as their provider's economic instability and local disasters, while evaluating cloud service providers. When data and procedures are moved to the cloud, the risk of an insider attack rises dramatically. Multi-tenant setups are particularly vulnerable to the effects of targeted attacks on one tenant, which can have severe ramifications for the other tenants in the building as a result. Risk analysis and management practices; penetration testing; service attestation must all be examined to guarantee that clients can reap the benefits of cloud computing [13]. Best practices and standards must be revisited to guarantee that secure clouds are adopted and deployed. Due to the worldwide nature of cloud computing, a well-structured cyber insurance market is exceedingly complicated[13]. Both cloud-specific and general IT industry trends will influence future cloud computing services and approaches to services, architectures, and innovation[11].
- **Increase in use of mobile devices:** Over the last few years, laptop sales have surpassed desktop sales, and this trend is expected to continue as an increasing number of mobile devices, such as notebooks, PDAs, and mobile phones, incorporate many of the features found on a desktop-based PC, such as Internet access and custom application functionality [11].
    1. Hardware capability improvements: The cloud will be able to serve increasingly complex environments with improved performance capabilities as a result of inevitable advancements in processing speed and memory capacity across IT infrastructure[11]..
    2. Tackling complexity: Despite the efforts of numerous technology vendors, this complexity challenge remains unresolved. IT architectures continue to be difficult to implement, underutilized, and expensive to operate. The massive scale of cloud computing only emphasizes the need for self-monitoring, self-healing, and self-

configuring IT systems comprised of heterogeneous storage, servers, applications, networks, and other system elements[14]..

3. Legislation and security: Vendors and providers will respond as larger firms examine the cloud computing paradigm, but only if their potential customers establish the terms. Because there are still many concerns with data privacy and data transfer over international borders, cloud service providers must continue to devote time and effort to comply with the regulations that govern some of their major clients' business sectors[13].

IV. Future work

Further research may be conducted in order to develop a software process model specifically for cloud computing related software development, which would resolve Security, Privacy, and Risk Issues beyond socio-cultural, economic, technological, and geographic constraints.

V. Conclusion

The fundamental reason why the future of cloud computing will be as powerful and expansive as it appears to be is the fact that the technology behind cloud computing offers a great deal of potential benefits. Cloud computing and the technology that enables it open the door to a plethora of opportunities and capabilities that were not previously available. Cloud computing has the ability to open up a whole new universe of options in terms of jobs, services, platforms, apps, and much more[10]. As the future of cloud computing gets off the ground, thousands of additional options are starting to become apparent. However, in order to fulfill all of society's requirements and also deftly handling future research issues, developers and service providers are obligated and should make it a priority to keep an eye on cloud computing provisions in the wider context of the trade[10].

References

[1]. https://www.bclplaw.com/images/content/3/1/v2/317141/2022-cloud-computing-united-kingdom.pdf
[2]. N. Afshan,"Analysis and Assessment of the Vulnerabilities in Cloud Computing," Int. J. Adv. Res. Comput. Sci., vol. 8, no. 2, 2017, pp. 2015–2018.
[3]. Cloud Security Alliance, "Best Practices for Mitigating Risks in Virtualized Environments," Downloads.cloudsecurityalliance.org, 2015. [Online].Available:https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%20_Mitigating-Risks _Virtual_Environments_April2015_4-1-15_GLM5.pdf. [Accessed: 11- Jan- 2017].
[4]. R. Schwarzkopf, (2015) "Virtual Machine Lifecycle Management in Grid and Cloud computing," University of Marburg. [Online]. Available: http://archiv.ub.unimarburg.de/diss/z2015/0407/pdf/ drs.pdf. [Accessed: Aug.-2017].
[5]. S. Z. I. Tariqul and D. Manivannan, "A Classification and Characterization of Security Threats in Cloud Computing," Int. J. Next-Generation Comput., vol. 7, no. 1, pp. 1–17, 2016.
[6]. C. N. Modi and K. Acha,"Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review," J. Supercomput., vol. 73, no. 3, 2017, pp. 1192-1234.
[7]. Moulika Bollinadi, Vijay Kumar Damera, "Cloud Computing: Security Issues and Research Challenges",Journal of Network Communications and Emerging Technologies (JNCET) www.jncet.org Volume 7, Issue 11, November (2017),pp.64-73.
[8]. Adesh Kumar,"Research Issues in Virtualization in Cloud Computing", International Journal of New Innovations in Engineering and Technology, Volume 12 Issue 4 January 2020,PP.149-159.
[9]. Rafat Ara1, Md. Abdur Rahim2, Sujit Roy3, Dr. Uzzal Kumar Prodhan4," Cloud Computing: Architecture, Services, Deployment Models, Storage, Benefits and Challenges", International Journal of Trend in Scientific Research and Development (IJTSRD) Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470.
[10]. https://data-flair.training/blogs/features-of-cloudcomputing/
[11]. https://www.javatpoint.com/cloud-computingarchitecture
[12]. https://www.w3schools.in/cloud-computing/cloudcomputing-architecture/
[13]. Dr.P.Sujatha, Dr.P.SriPriya," Security Threats and Preventive Mechanisms in Cloud Computing", Journal of Applied Science and Computations , ISSN NO: 1076- 5131,Volume V, Issue XII, December/2018, page no. 2112-2119.
[14]. Bahrami, A., & Harish Babu, S. (2020). Migration to cloud computing-changing paradigm in Indian IT sector. International Journal of Scientific and Technology Research, 9(4), 292– 299. Scopus.
[15]. Damera, V. K., Nagesh, A., & Nagaratna, M. (2020). Trust evaluation models for cloud computing. International Journal of Scientific and Technology Research, 9(2), 1964–1971. Scopus.
[16]. NIST Cloud Computing Standards Roadmap (SP 500-291).p.p 1-23