In-depth Analysis of Cloud Computing Architectures, Deployment Models, Security Issues, Virtualization Technologies, and Cloud-Based Services

Vicrumnaug Vuppalapaty

Technical Architect, CodeScience Inc. USA

Abstract:

Cloud computing is the development of parallel computing, distributed computing, grid computing and virtualization technologies which define the shape of a new era. Cloud computing is an emerging model of business computing. In this paper, we explore the concept of cloud architecture and compare cloud computing with grid computing. We also address the characteristics and applications of several popular cloud computing platforms. In this paper, we aim to pinpoint the challenges and issues of cloud computing. We identified several challenges from the cloud computing adoption perspective and we also highlighted the cloud interoperability issue that deserves substantial further research and development. However, security and privacy issues present a strong barrier for users to adapt into cloud computing systems. In this paper, we investigate several cloud computing system providers about their concerns on security and privacy issues.

Keywords— Cloud computing, architecture, challenges, cloud platforms, research issues.

INTRODUCTION

Cloud computing is a complete new technology. It is the development of parallel computing, distributed computing grid computing, and is the combination and evolution of Virtualization, Utility computing, Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS)[1]. Cloud is a metaphor to describe the web as a space where computing has been pre-Installed and exists as a service; data, operating systems, applications, storage and processing power exist on the web ready to be shared. To users, cloud computing is a Pay-per-Use-On-Demand mode that can conveniently access shared IT resources through the Internet. Where the IT resources include network, server, storage, application, service and so on and they can be deployed with much quick and easy manner and least management and also interactions with service providers[2]. Cloud computing can greatly improve the availability of IT resources and has many advantages over other computing techniques. Users can use the IT infrastructure with Pay-per-Use-On-Demand mode; this would benefit and save the cost to buy the physical resources that may be vacant[2].

Organization. The rest of the paper is organized as follows: In Section II, we define architectural components such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Data as a Service (DaaS). Then, we compare cloud and grid computing in Section III and explain some popular cloud computing platforms in Section IV. In Section V, we include a few applications of cloud computing[3]. We further explained about issues and challenges of cloud computing in Section VI, VII and VIII. Finally, we conclude in Section IX.

ARCHITECTURAL COMPONENTS

Cloud service models are commonly divided into SaaS, PaaS, and IaaS that are exhibited by a given cloud infrastructure. It's helpful to add more structure to the service model stacks: Fig. 1 shows a cloud reference architecture [13] that makes the most important security-relevant cloud components explicit and provides an abstract overview of cloud computing for security issue analysis.

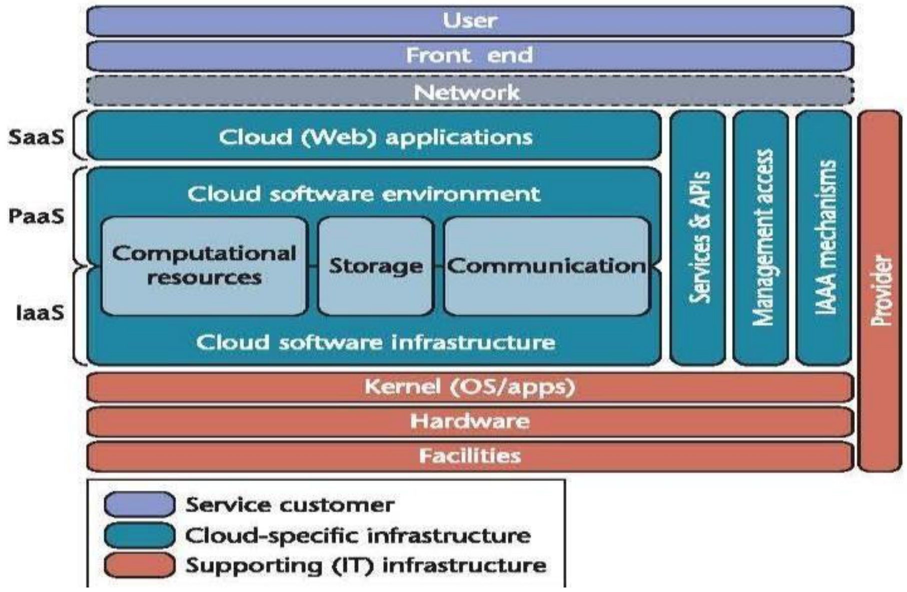

Fig. 1. The cloud reference architecture.

A. Software as a Service (SaaS)

Cloud consumers release their applications in a hosting environment, which can be accessed through networks from various clients (e.g. Web browser, PDA, etc.) by application users. Cloud consumers do not have control over the cloud infrastructure that often employs multi-tenancy system architecture, namely, different cloud consumers' applications are organized in a single logical environment in the SaaS cloud to achieve economies of scale and optimization in terms of speed, security, availability, disaster recovery and maintenance[4]. Examples of SaaS include SalesForce.com, Google Mail, Google Docs, and so forth.

B. Platform as a Service (PaaS)

PaaS is a development platform supporting the full "Software Lifecycle" which allows cloud consumers to develop cloud services and applications (e.g. SaaS) directly on the PaaS cloud. Hence, the difference between SaaS and PaaS is that SaaS only hosts completed cloud applications whereas PaaS offers a development platform that hosts both

Completed and in-progress cloud applications.[5] This requires PaaS, in addition to supporting application hosting environments, to possess development infrastructure including programming environment, tools, configuration management, and so forth. An example of PaaS is Google App Engine.

C. Infrastructure as a Service (IaaS)

Cloud consumers directly use IT infrastructures (processing, storage, networks and other fundamental computing resources) provided in the IaaS cloud[6]. Virtualization is extensively used in IaaS cloud in order to integrate/decompose physical resources in an ad-hoc manner to meet growing or shrinking resource demand from cloud consumers. The basic strategy of virtualization is to set up independent virtual machines (VM) that are isolated from both the underlying hardware and other VMs[6]. Notice that this strategy is different from the multi-tenancy model, which aims to transform the application software architecture so that multiple instances (from multiple cloud consumers) can run on a single application (i.e. the same logic machine). An example of IaaS is Amazon's EC2.

D. Data as a Service (DaaS)

The delivery of virtualized storage on demand becomes a separate Cloud service data storage service[7]. Notice that DaaS could be seen as a special type of IaaS. The motivation is that on-premise enterprise database systems are often tied in a prohibitive upfront cost in dedicated server, software license, post-delivery services and in-house IT maintenance. DaaS allows consumers to pay for what they are actually using rather than the site license for the entire database[8]. In addition to traditional storage interfaces such as RDBMS and file systems, some DaaS offerings provide table-style abstractions that are designed to scale out to store and retrieve a huge amount of data within a very compressed timeframe, often too large, too expensive or too slow for most commercial RDBMS to cope with. Examples of this kind of DaaS include Amazon S3, Google Big Table, and Apache HBase, etc.

COMPARISON BETWEEN CLOUD AND GRID COMPUTING

A comparison [6] can be summarized as follows:

1) Construction of the grid is to complete a specified task, such as biology grid, Geography grid, national educational grid, while Cloud computing is designed to meet general application and there is no grid for a special field.

2) Grid emphasizes the “resource sharing” to form a virtual organization. Cloud is often

owned by a single physical organization (except the community Cloud, in this case, it is owned by the community), who allocates resources to different running instances.

3) Grid aims to provide the maximum computing capacity for a huge task through resource sharing. Cloud aims to suffice as many small-to-medium tasks as possible based on users' real-time requirements. Therefore, multi-tenancy is a very important concept for Cloud computing. Grid trades re-usability for (scientific) high performance computing. Cloud computing is directly pulled by immediate user needs driven by various business requirements.

4) Grid strives to achieve maximum computing[8]. Cloud is after on-demand computing – Scale up and down, in and out at the same time optimizing the overall computing capacity.

POPULAR CLOUD COMPUTING PLATFORMS

A. AbiCloud

AbiCloud [5] is a cloud computing platform. It can be used to build, integrate and manage public as well as private cloud platforms in homogeneous environments[9]. Using the AbiCloud, users can easily and automatically deploy and manage the server, storage system, network, virtual devices and applications and so on. The main difference between AbiCloud and other cloud computing platforms is its powerful web-based management function and its core encapsulation manner. Using the AbiCloud, users can finish deploying a new service by just dragging a virtual machine with a mouse[10]. This is much easier and flexible than other cloud computing platforms that deploy new services through command lines.

AbiCloud can be used to deploy and implement private cloud as well as hybrid cloud according to the cloud providers' request and configuration.[11] It can also manage EC2 according to the rules of protocol. Besides, apply the AbiCloud, a whole cloud platform based on AbiCloud can be packed and redeployed at any other AbiCloud platform. This is much helpful for the transformation of the working environment and will make the cloud deployment process much easier and flexible.

B. Eucalyptus

Eucalyptus (Elastic Utility Computing Architecture for Linking Your Programs to Useful Systems) [5] mainly was used to build open-source private cloud platforms [12]. Eucalyptus is an elastic computing structure that can be used to connect the users' programs to the useful systems, it is an open-source infrastructure using clusters or workstation implementation of elastic, utility, cloud computing and a popular computing standard based on a service level protocol that permit users lease network for computing capability[13].

Currently, Eucalyptus is compatible with EC2 from Amazon, and may support more other kinds of clients with minimum modification and extension.

C. Nimbus

Nimbus [5] is an open tool set and also a cloud computing solution providing IaaS. It permits users to lease remote resources and build the required computing environment through the deployment of virtual machines.[14] Generally, all these functional components can be classified as three kinds. One kind is client- supported modules which are used to support all kinds of cloud clients. Context client module, cloud client module, reference client module and EC2 client module are all belonging to this kind of component [15]t. The second kind of component is mainly Service-supported modules of cloud platform, providing all kinds of cloud services. It includes a context agent module, web service resource framework module, EC2 WSDL module and a remote interface module [16]. The third kind of component is the background resource management modules which are mainly used to manage all kinds of physical resources on the cloud computing platform, including work service management module, IaaS gateway module, EC2 and other cloud platform support module, workspace pilot module, workspace resource management module and workspace controller.

D. OpenNebula

OpenNebula [5] is also an open source cloud service framework. It allows user deploy and manage virtual machines on physical resources and it can set user's data centers or clusters to flexible virtual infrastructure that can automatically adapt to the change of the service load[17]. The main difference between OpenNebula and Nimbus is that Nimbus implements a remote interface based on EC2 or WSRF through which users can process all security related issues, while OpenNebula does not. OpenNebula is also an open and flexible virtual infrastructure management tool, which can be used to synchronize the storage, network and virtual techniques and let users dynamically deploy services on the distributed infrastructure according to the allocation strategies for data center and remote cloud resources[18]. Through the interior interfaces and OpenNebula data center environment, users can easily deploy any type.

TABLE I: THE COMPARISON OF SERVER CLOUD COMPUTING PLATFORMS [5]

	AbiCloud	Eucalyptus	Nimbus	OpenNebula
Cloud Character	Public/private	Public	Public	Private
Scalability	Scalable	Scalable	Scalable	Dynamic, Scalable
Clouds form	IaaS	IaaS	IaaS	IaaS
Compatibility	Not support EC2	Support EC2, S3	Support EC2	Open, multi-platform
Deployment	Pack and redeploy	Dynamical deployment	Dynamical deployment	Dynamical deployment
Deployment Manner	Web interface drags	Command line	Command line	Command line
Transplant-ability	Easy	Common	Common	Common
VM support	Virtual Box, Xen, VMware,	Xen, VMware, KVM	Xen	Xen, VMware

	VM			
Web interface	Libvirt	Web service	EC2, WSDL, WSRF	libvirt, OCCI, EC2, API
Structure	Open platform encapsulates core	Module	Lightweight components	Module
Reliability	-	-	-	Rollback host and VM
OS support	Linux	Linux	Linux	Linux
Development language	Ruby, c++, python	Java	Java, python	Java

APPLICATIONS

There are a few applications of cloud computing [4] as follows:

1. Cloud computing provides a dependable and secure data storage center.
2. Cloud computing can realize data sharing between different equipment.
3. The cloud provides nearly infinite possibilities for users to use the internet.
4. Cloud computing does not need high quality equipment for the user and it is easy to use.

ISSUES IN CLOUD COMPUTING

More and more information on individuals and companies is placed on the cloud; and thus, concerns are beginning to grow about just how safe this environment is for its users? Issues of cloud computing [3] can summarize as follows:

A. Privacy

Cloud computing utilizes the virtual computing technology, users' personal data may be scattered in various virtual data centers rather than stay in the same physical location, users may leak hidden information when they are accessed cloud computing services [19]. Attackers can analyze the critical task depending on the computing task submitted by the users.

B. Reliability

The cloud servers also experience downtimes and slowdowns as our local server.

C. Legal Issues

Worries stick with safety measures and confidentiality of individuals all the way through legislative levels.

D. Compliance

Numerous regulations pertaining to the storage and use of data requires regular reporting and audit trails[19]. In addition to the requirements to which customers are subject, the data centers maintained by cloud providers may also be subject to compliance requirements.

E. Freedom

Cloud computing does not allow users to physically possess the storage of the data, leaving the data storage and control in the hands of cloud providers.

F. Long- Term Viability

You should be sure that the data you put into the cloud will never become invalid even if your cloud computing provider goes broke or gets acquired and swallowed up by a larger company.

G. Issues in Cloud Interoperability

1) Intermediary Layer

A number of recent works address the interoperability issue by providing an intermediary layer between the cloud consumers and the cloud-specific resources (e.g. VM).

2) Open Standard

Standardization appears to be a good solution to address the interoperability issue[20]. However, as cloud computing just starts to take off, the interoperability problem has not appeared on the pressing agenda of major industry cloud vendors.

3) Open API

SUN has recently introduced the Sun Open Cloud Platform [10], released under the Creative Commons license [21]. A key feature of this platform is the proposed cloud API, which is currently under development [22]. This API offers a set of clear and intuitive RESTful Web services interfaces, enabling cloud consumers to efficiently create and manage cloud resources such as compute, storage, and networking components in a unified manner.

4) SaaS and PaaS Interoperability

While the aforementioned solutions generally tackle IaaS interoperability problems,[23] SaaS interoperability often involves different application domains such as ERP, CRM, etc. A group of experts in the field of data mining raises the issue of establishing a data mining standard on the cloud, with a particular focus on "the practical use of statistical algorithms, reliable production deployment of models and the integration of predictive analytics" across different data mining-based SaaS clouds.[24]

PaaS interoperability not yet discovered Since PaaS involves the entire software development life-cycle on the cloud, it would be more difficult to reach uniformity with regards to the way consumers develop and deploy cloud applications.

CHALLENGES ON CLOUD ADOPTION PERSPECTIVE based on a survey conducted by IDC in 2008

A. Security

Well-known security issues such as data loss, phishing, and botnets (running remotely on a collection of machines) pose serious threats to an organization's data and software[25]. The multi - tenancy model and the pooled computing resources on cloud computing has introduced new security challenges such as shared resources (hard disk, data, VM) on the same physical machine that invites unexpected side channels between a malicious resource and a regular resource[26]. And, the issue of "reputation fate-sharing" will severely damage the reputation of many good Cloud "citizens" who happen to, unfortunately, share the computing resources with their fellow tenant - a notorious user with a criminal mind. Since they may share the same network address, any bad conduct will be attributed to all the users without differentiating real subverts from normal users.

B. Costing Model

Cloud consumers must consider the tradeoffs amongst computation, communication, and integration[26]. While migrating to the Cloud can significantly reduce the infrastructure cost, it does raise the cost of data communication.

C. Charging Model

From a cloud provider's perspective, the elastic resource pool (through either virtualization or multi-tenancy) has made the cost analysis a lot more complicated than regular data centers, which often calculates their cost based on consumptions on static computing.

D. Service Level Agreement

It is vital for consumers to obtain guarantees from providers on service delivery. Typically, these are provided through Service Level Agreements (SLAs) negotiated between the providers and consumers[27].

A Service Level Agreement (SLA) in cloud computing is a contractual commitment between a cloud service provider and its customers, outlining the performance and reliability metrics that the provider agrees to meet[27]. This agreement serves as a crucial component in establishing trust and accountability in the cloud computing environment.

Performance Metrics: SLAs typically specify various performance metrics, including uptime, response time, and availability. For instance, an SLA might guarantee that the cloud services will be available 99.9% of the time (often referred to as "three nines" availability)[28]. This ensures that customers can rely on consistent and uninterrupted access to their applications and data hosted on the cloud platform.

Response Time: Response time is another critical metric covered in an SLA, which refers to the time it takes for the cloud service to respond to a user request. A well-defined SLA will specify acceptable response times for different types of operations and transactions, ensuring that the cloud services meet the performance expectations of the customers.

Data Security and Privacy: SLAs also address data security and privacy concerns by outlining the measures the provider will take to protect customer data[28]. This may include encryption protocols, data backup procedures, and compliance with relevant data protection regulations such as GDPR or CCPA. The SLA should provide assurance to the customers that their data will be handled with the utmost confidentiality and integrity.

Scalability and Flexibility: Cloud services are expected to be scalable and flexible to accommodate the changing needs of businesses. Therefore, an SLA should specify the provider's commitment to scalability, ensuring that the infrastructure can handle increased workloads and resource demands without compromising performance or reliability.

Disaster Recovery and Business Continuity: SLAs often include provisions related to disaster recovery and business continuity, detailing the provider's strategies and procedures for mitigating the impact of potential disruptions or failures. This may involve regular data backups, failover mechanisms, and recovery time objectives (RTO) and recovery point objectives (RPO) to minimize downtime and data loss.

Compliance and Governance:Lastly, SLAs should address compliance and governance requirements, ensuring that the cloud services comply with industry regulations and standards. This may include certifications such as ISO 27001 for information security management or SOC 2 for data privacy and protection[28]. A well-crafted Service Level Agreement (SLA) in cloud computing is essential for establishing clear expectations, responsibilities, and safeguards for both the cloud service provider and the customer[29]. It serves as a contractual assurance of reliability, performance, security, and compliance, enabling businesses to leverage the benefits of cloud computing with confidence and peace of mind.

SECURITY AND PRIVACY ISSUE

Cloud computing can provide infinite computing resources on demand due to its high scalability in nature, which eliminates the need for Cloud service providers to plan far ahead on hardware provisioning. Many companies, such as Amazon, Google, Microsoft and so on, accelerate their pace in developing cloud computing systems and enhancing their services to a larger number of users.

In this paper, we investigate the security and privacy concerns of current cloud computing systems provided by an amount of companies. Cloud computing refers to both the applications delivered as services over the Internet and the infrastructures (i.e., the hardware and systems software in the data centers) that provide those services[29]. Based on the investigation, security and privacy concerns provided by companies nowadays are not adequate, and consequently result in a big obstacle for users to adapt into the cloud computing systems. Hence, more concerns on security issues, such as availability, confidentiality, data integrity, control, and audit and so on, should be taken into account.

A. Security on Demand

Cloud services are applications running somewhere in the cloud computing infrastructures through internal network or Internet. Cloud computing allows providers to develop, deploy and run applications that can easily grow in capacity (scalability), work rapidly (performance), and never (or at least rarely) fail (reliability), without any concerns on the properties and the locations of the underlying infrastructures[29]. Cloud computing systems can achieve the following five goals together [2] In today's fast-paced and interconnected digital landscape, the need for robust and adaptive security solutions has never been more critical. "Security on Demand" represents a dynamic and responsive approach to safeguarding your organization's valuable assets and data. This multifaceted strategy leverages cutting-edge technologies, continuous monitoring, and rapid response mechanisms to counteract a wide array of cyber threats. By offering scalability and flexibility, Security on Demand ensures that your security measures can evolve in tandem with your business needs and the ever-changing threat landscape. Whether it's protecting sensitive information, ensuring regulatory compliance, or defending against sophisticated cyber-attacks, a comprehensive Security on Demand solution provides the peace of mind and resilience that modern enterprises require[29]. Cloud computing offers numerous benefits, including scalability, flexibility, and cost-efficiency, but it also introduces a range of security and privacy concerns that organizations must address to safeguard their data and operations effectively.

Data Breaches and Unauthorized Access: One of the primary security concerns in cloud computing is the risk of data breaches and unauthorized access. Storing sensitive or confidential data in the cloud can make it a target for cybercriminals seeking to exploit vulnerabilities in the cloud infrastructure or applications [29]. Therefore, robust security measures, such as encryption, access controls, and multi-factor authentication, are essential to protect data integrity and confidentiality.

Compliance and Regulatory Challenges: Compliance with various industry regulations and data protection laws, such as GDPR, CCPA, and HIPAA, is another significant issue in cloud computing. Cloud service providers must ensure that their services adhere to these regulations, which often require specific data handling and protection measures. Failure to comply can result in severe legal consequences and reputational damage for both the provider and the customer.

Data Loss and Recovery: Data loss is a critical concern in cloud computing due to factors such as hardware failures, software bugs, or human error[30]s. While cloud providers typically implement backup and disaster recovery solutions, customers must still ensure that their data is adequately protected and that they have access to backup copies when needed. Recovery time objectives (RTO) and recovery point objectives (RPO) should be clearly defined in the Service Level Agreement (SLA) to minimize the impact of potential data loss incidents.

Shared Resources and Multi-tenancy Risks: Cloud computing often involves shared resources and multi-tenancy environments, where multiple customers share the same infrastructure and resources. This shared environment can potentially expose organizations to risks such as cross-tenant data breaches, where one tenant's data is accessed or compromised by another. To mitigate these risks, cloud providers must implement robust isolation mechanisms and security controls to prevent unauthorized access between different tenants.

Insider Threats: Insider threats, including malicious activities by employees, contractors, or third-party service providers with access to the cloud environment, pose a significant security risk. Organizations must implement strict access controls, monitoring, and auditing mechanisms to detect and prevent insider threats effectively. Employee training and awareness programs can also help mitigate the risk of unintentional data breaches caused by human errors or negligence.

Lack of Transparency and Control: The lack of transparency and control over the cloud infrastructure and security practices can also be a concern for organizations using cloud services. Customers often have limited visibility into the provider's security measures, data handling processes, and compliance practices. To address this issue, cloud providers should offer transparency through regular audits, compliance certifications, and clear communication about their security and privacy practices.

1) Availability

The goal of availability for cloud computing systems (including applications and its infrastructures) is to ensure its users can use them at any time, at any place. As its web-native nature, cloud computing system enables its users to access the system (e.g., applications, services) from anywhere [30]. This is true for all cloud computing systems (e.g., DaaS, SaaS, PaaS, IaaS, and etc.). Required to be accessed at any time, the cloud computing system should be serving all the time for all the users (say it is scalable for any number of users). Two strategies, say hardening and redundancy, are mainly used to enhance the availability of the cloud system or applications hosted on it.

2) Confidentiality

It means keeping users' data secret in the cloud systems. There are two basic approaches (i.e., physical isolation and cryptography) to achieve such confidentiality, which are extensively adopted by the cloud computing vendors.

3) Data integrity

In the cloud system means to preserve information integrity (i.e., not lost or modified by unauthorized users). As data are the base for providing cloud computing services, such as Data as a Service, Software as a Service, Platform as a Service, keeping data integrity is a fundamental task.

4) Control

In the cloud system means to regulate the use of the system, including the applications, its infrastructure and the data.

5) Audit

It means to watch what happened in the cloud system. Auditability could be added as an additional layer in the virtualized operating system (or virtualized application environment) hosted on the virtual machine to provide facilities for monitoring as to what happened in the system. It is much more secure than that is built into the applications or into the software themselves, since it is able to assess the entire access duration.

CONCLUSION

This paper discussed the architecture and popular platforms of cloud computing. It also addressed challenges and issues of cloud computing in detail. In spite of the several limitations and the need for better methodologies processes, cloud computing is becoming a hugely attractive paradigm, especially for large enterprises. Cloud Computing initiatives could affect the enterprises within two to three years as it has the potential to significantly change IT. Certainly, here's a conclusion paragraph that summarizes the issues, challenges, architecture, platforms, and applications in cloud computing:

In conclusion, cloud computing has revolutionized the way organizations develop, deploy, and manage applications by offering scalability, performance, reliability, flexibility, and cost-efficiency. However, it is not without its challenges and issues. Security and privacy concerns remain at the forefront, requiring robust solutions to safeguard data and ensure compliance with regulations. Additionally, interoperability, portability, and vendor lock-in issues can limit flexibility and hinder migration between different cloud platforms. On the architecture front, cloud computing typically involves a layered architecture comprising Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), each offering varying levels of abstraction and control over the underlying infrastructure. Various cloud platforms such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP) have emerged as dominant players in the market, each providing a comprehensive set of services and features to meet diverse business needs.

Furthermore, cloud computing applications span a wide range of domains, including but not limited to, data analytics, artificial intelligence, Internet of Things (IoT), and machine learning. These applications leverage the scalability and computational power of the cloud to process and analyze large volumes of data, derive valuable insights, and enable innovative solutions across industries. Despite the challenges, the continuous advancements in cloud computing technologies, coupled with the growing demand for digital transformation and agile business operations, are driving the adoption and evolution of cloud-based solutions. As organizations continue to embrace cloud computing, addressing the existing challenges, understanding the architecture, selecting the appropriate platforms, and leveraging cloud-based applications will be crucial for realizing the full potential of cloud computing and achieving strategic business objectives.

REFERENCES

1. T. Dillon, C. Wu, and E. Chang, "Cloud Computing: Issues and Challenges," *2010 24th IEEE International Conference on Advanced Information Networking and Applications(AINA)*, pp. 27-33, DOI= 20-23 April 2010
2. M. Q. Zhou, R. Zhang, W. Xie, W. N. Qian, and A. Zhou, "Security and Privacy in Cloud Computing: A Survey," *2010 Sixth InternationalConference on Semantics, Knowledge and Grids(SKG)*, pp.105-112,
3. DOI= 1-3 Nov. 20 10
4. J. F. Yang and Z. B. Chen, "Cloud Computing Research and Security Issues," *2010 IEEE International Conference on Computational Intelligence and Software Engineering (CiSE)*, Wuhan pp. 1-3, DOI= 10-12 Dec. 2010.
5. S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "Cloud Computing Research and Development Trend," In *Proceedings of the 2010 Second International Conference on Future Networks* (ICFN '10). IEEE Computer Society, Washington, DC, USA, pp. 93-97. DOI=10.1109/ICFN.2010. 58.
6. J. J. Peng, X. J. Zhang, Z. Lei, B. F. Zhang, W. Zhang, and Q. Li, "Comparison of Several Cloud Computing Platforms," *2009 Second International Symposium on Information Science and Engineering (ISISE '09)*. IEEE Computer Society, Washington, DC, USA, pp. 23-27, DOI=10.1109/ISISE.2009.94.
7. S. Zhang, S. F. Zhang, X. B. Chen, and X. Z. Huo, "The Comparison between Cloud Computing and Grid Computing," *2010 International Conference on Computer Application and System Modeling (ICCASM)*, pp. V11-72 - V11-75, DOI= 22-24 Oct. 2010.
8. M. M. Alabbadi, "Cloud Computing for Education and Learning: Education and Learning as a Service (ELaaS)," *2011 14th International Conference on Interactive Collaborative Learning (ICL)*, pp. 589 – 594, DOI=21-23 Sept. 2011.
9. P. Kalagiakos "Cloud Computing Learning," *2011 5th International Conference on Application of Information and Communication Technologies (AICT)*, Baku pp. 1 - 4, DOI=12-14 Oct. 2011.
10. P. Mell and T. Grance, "Draft nist working definition of cloud computing - vol. 21, Aug 2009, 2009.
11. "Sun Microsystems Unveils Open Cloud Platform," [Online]. Available:

12. http://www.sun.com/aboutsun/pr/2009-03/sunflash.20090318.2.xml,2 009.

13. W. Dawoud, I. Takouna, and C. Meinel, "Infrastructure as a Service Security: Challenges and Solutions," *2010 7th International Conference on Informatics and System*, pp. 1-8, March 2010.

14. W. Itani, A. Kayssi, and A. Chehab, "Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures," *2009 8th IEEE International Conference on Dependable, Autonomic and Secure Computing*, 2009, pp. 711-716.

15. B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding Cloud Computing Vulnerabilities," *2011 IEEE Security and Privacy*, pp. 50-57, DOI= March/April 2011.

16. W. A. Jansen, "Cloud Hooks: Security and Privacy Issues in Cloud Computing," *Proceedings of the 44th Hawaii International Conference on System Sciences*, 2011.

17. Almond, Carl., "A practical guide to cloud computing security," A white paper from Accenture and Microsoft, pp. 3-9, 2009.

18. Basson, Benhardus., "The right to privacy: how the proposed POPI Bill will impact data security in a Cloud Computing environment," PhD theisis., Stellenbosch:Stellenbosch University, pp. 1-67, 2014.

19. Srinivasamurthy, Shilpashree, D. Liu., "Survey on Cloud Computing Security," In Proc. Conf. on Cloud Computing, Cloud Com, vol. 10. Pp. 412-421, 2010.

20. Dillon, Tharam, C. Wu, E. Chang," Cloud computing: issues and challenges," In Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on, pp. 27-33. IEEE, 2010

21. Singhal, Paridhi., "Data Security Models in Cloud Computing," International Journal of Scientific & Engineering Research, Vol. 4, No. 6, pp. 789-793, Jun. 2013.

22. Carlin, Sean, K. Curran., "Cloud computing security," International Journal of Ambient Computing and Intelligence (IJACI) 3, no. 1, pp. 14-19, 2011. Article (CrossRef Link)

23. Srivastava, Prashant, S. Singh, A. Alfred Pinto, S. Verma, Vijay K. Chaurasiya, Rahul Gupta., "An architecture based on proactive model for security in cloud computing," In Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, pp. 661-666. IEEE, 2011.

24. Al-Anzi, Fawaz S., Sumit Kr Yadav, J. Soni, "Cloud computing: Security model comprising governance, risk management and compliance," In Data Mining and

Intelligent Computing (ICDMIC), 2014International Conference on, pp. 1-6. IEEE, 2014

25. Blakstad, Kåre Marius, M. Andreassen., "Security in Cloud Computing: A Security Assessment of Cloud Computing Providers for an Online Receipt Storage," pp. 1- 103, 2010.
26. Padhy, Rabi Prasad, M. R. Patra, S. Chandra Satapathy., "Cloud Computing: Security Issues and Research Challenges," International Journal of Computer Science and Information Technology &Security (IJCSITS) 1, no. 2, pp. 136-146, 2011.
27. Khalil, Issa M., A. Khreishah, S. Bouktif, A. Ahmad., "Security concerns in cloud computing," In Information Technology: New Generations (ITNG), 2013 Tenth International Conference on, IEEE, pp. 411-416, 2013. Article (CrossRef Link)
28. Mewed, Shiva Zhang, Rui, Ling Liu., "Security models and requirements for healthcare application clouds," In Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, pp. 268-275. IEEE, 2010.
29. U. Kumar Singh, P. Sharma., "Security Based Model for Cloud Computing," Int. Journal of Computer Networks and Wireless Communications (IJCNWC) 1, no. 1, pp. 13-19, 2011.
30. Vaquero, LuisM., L. R. –M, Daniel Morán., "Locking the sky: a survey on IaaS cloud security," Computing 91, no. 1, pp. 93-118, 2011. Article (CrossRef Link)
31. Aliabad, Mohsen M., "Cloud computing for education and learning: Education and learning as a service(ELaaS)," In Interactive Collaborative Learning (ICL), 2011 14th International Conference on, pp. 589-594. IEEE, 2011.
32. Vijay.G.R, Dr.A.Rama Mohan Reddy., "Investigational Analysis of Security Measures Effectiveness in Cloud Computing: A Study," Computer Engineering and Intelligent Systems, Vol.5, No.7, pp 23-30, 2014