A Comprehensive Analysis of Core Characteristics, Service Models, and Data Integrity Mechanisms for Secure Cloud Computing

Aaron Mike Oquaye
University of Professional Studies, Madina, Ghana.
aaron.oquaye@upsamail.edu.gh

John Atta Mills
University of Professional Studies, Madina, Ghana.
attamills1@outlook.com

Article Info
Journal of Computer and Communication Networks
https://www.ansispublications.com/jccn /jccn.html

Received 18 January 2025
Revised from 02 March 2025
Accepted 30 April 2025
Available online 22 May 2025
Published by Ansis Publications

https://doi.org/10.64026/JCCN/2025011

Corresponding author(s):
John Atta Mills, University of Professional Studies, Madina, Ghana.
Email: attamills1@outlook.com

Abstract – The article describes the environment of cloud computing and gives a detailed explanation of its key characteristics, types of services, and the issue of data security. The study starts with the definition of cloud computing and its main principles, including the service-oriented model and combined structure of the architecture. These characteristics make it possible to use existing resources effectively and increase the scale of operations. This article provides a proper description of the various service models that are offered by cloud providers such as Platform as a Service (PaaS), Infrastructure as a Service (IaaS) and Software as a Service (SaaS). These frameworks are all intended to meet the perceived needs and desires of different users. In addition, the study presents the economic perspective of cloud computing and how it is affected by the business models that are associated with pay-as-you-go and utility computing. Besides, the research provides an understanding of the problem of data integrity in cloud environments, along with such questions as data and the reliability of calculations made on remote servers. Consequently, this research seeks to advance the knowledge on the dynamics of cloud computing by offering an improved understanding of these facets. In addition, it is expected to offer relevant information that can improve the security and dependability of cloud computation in practical application.

Keywords – Platform-as-a-Service, Infrastructure-as-a-Service, Software-as-a-Service, Cloud Computing, Service-Oriented Structure.

I. INTRODUCTION

Cloud computing is slowly becoming a leading trend where many current and developing organizations are considering to seek assistance as it holds the promise of bringing about cheaper development and maintenance while providing highly reliable and efficient services. Cloud technology is an emerging process that is currently in the experimentation phase. The cloud has several economic benefits and flexibility and expansibility for businesses [1]. Organizational software and data are stored in distant facilities termed as data centers, which enhance the ability of organizations to deliver programs at a faster rate with better control and less demand for attention. Also, it enables one to increase or decrease resources such as storage, servers and networking in tandem with the needs of the firm. In a cloud setting, a data center stores data, which could otherwise be stored on the individual users' machines. This raises issues over the preservation of user privacy since users are required to entrust their data to other sources [2]. The migration of information to centralized cloud services has the potential to impact the security and privacy of interactions by users with records stored in the cloud server. Utilizing virtualized system as a starting point may expose user data to new forms of attacks. Data integrity refers to the precision and uniformity of recorded data, without any modifications to the contents between two updates of a file or record.

Cloud computation has arisen as a salient technological trend, with analysts predicting that it will essentially transform information technology (IT) trials and the IT industry. Cloud computation technology enables users to access plans, storage, and utilization-advancement stages via the Internet using a variety of gadgets such as laptops, PCs, cellphones, and PDAs. These services are given by cloud computation providers. The benefits of cloud computation technologies include reduced expenses, increased availability, and easy scalability. Botta et al. [3] categorizes cloud services into three distinct groups, as seen in **Fig. 1**. **Fig. 1a** depicts the cloud service SaaS, in which the whole utilization operates inside the cloud. The client includes a basic web browser for accessing the program. One widely known instance of Software as a Service (SaaS) is salesforce.com. **Fig. 1b** depicts an alternative form of cloud services, in which the utilization is executed on the client side but utilizes beneficial purposes and facilities offered in the cloud. An instance of this kind of cloud services available on personal computers is Apple's iTunes. The desktop program functions as a music player, while the cloud service is used for the acquisition of fresh video and audio material. Microsoft Exchange Hosted Services is a prime example of this type of cloud solution for enterprises. The on-premises Exchange Server makes use of additional cloud-based services for things like archiving and spam filtering, among other features. **Fig. 1** depicts a cloud service used by developers to create apps. The developers construct a novel SaaS utilization using the cloud service.

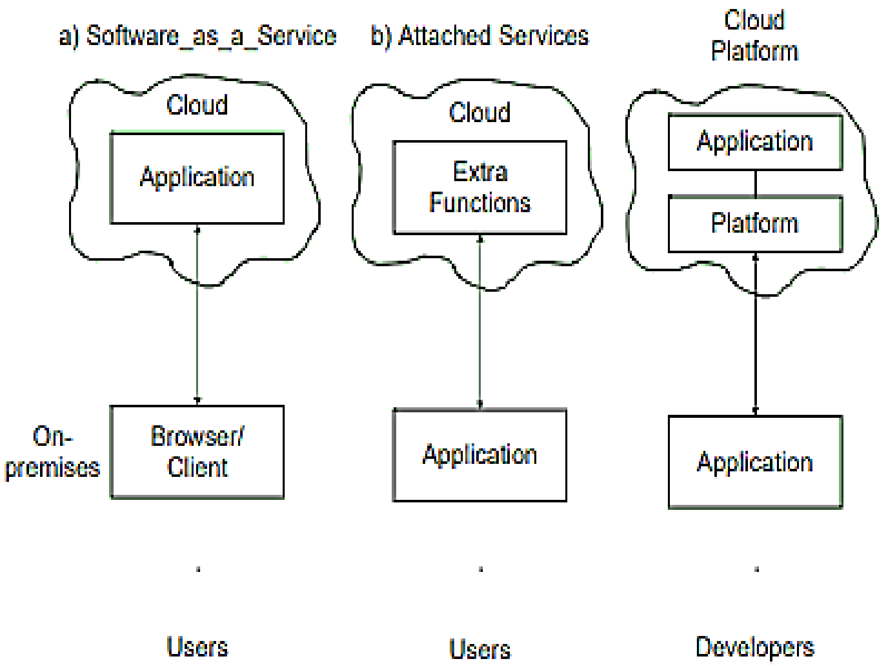

Fig 1. The Groups of Cloud Services.

Cloud services must guarantee the integrity of data and prioritize customer privacy. While the economic benefits of outsourcing data to the cloud for long-term, large-scale storage are appealing, the absence of clear guarantees regarding data quality and availability may hinder its widespread adoption by both company and individual cloud users [4]. The main privacy problems associated with cloud computing arise from the fact that the service giver has the potential to access the data stored in the cloud at any given moment. The cloud service giver has the potential to unintentionally or intentionally modify or erase some data stored on the cloud server. Therefore, the system must provide a method to guarantee the integrity of the data. The existing Cloud security approach operates on the premise that the user/customer must place faith in the provider. Typically, a Service Level Agreement (SLA) governs this process, outlining the expectations and duties of both the supplier and the user. To guarantee the dependability and accessibility of data in the Cloud and enforce the excellence of cloud storage service, it is necessary to develop effective techniques that allow cloud users to verify data accuracy whenever needed. Nevertheless, the absence of physical ownership of data by users in the cloud hinders the direct use of conventional cryptographic methods to ensure data integrity [5].

This research seeks to highlight the increasing importance of cloud computing by exploring its fundamental features, service models, and concerns of data authenticity. Given the growing prevalence of cloud technologies in many industries, it is essential for professionals, scholars, and policymakers to have a comprehensive awareness of these factors. This research aims to clarify the basic principles and possible weaknesses of cloud computing, which is vital in providing information for decision-making, improving security measures, and contributing to the development of more resilient and dependable cloud computing technologies for use in real-world situations.

The subsequent sections of this study have been arranged as follows: Section II discusses the characteristics of cloud computing, which integrates national features (service aligned), mechanical feature 1 and 2 (loose connection and strong fault tolerance), monetary feature (business framework), and user practice feature (ease use). Section III describes the service models such as Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). Section IV describes different deployment models, such as private cloud, community cloud, hybrid cloud, public cloud, virtual private cloud, and inter-cloud. Section V reviews the various data integrity issues such as data loss or manipulations, and untrusted remote server calculating user behaviors. Section VI summarizes the paper, and provides directions for future research.

II. CHARACTERISTIC OF CLOUD COMPUTING

Data center computing, supercomputing, high performance computing (HPC), cloud computation, and grid computation are all forms of parallel computing. HPC is primarily concerned with scientific computing, which involves computationally demanding tasks that need low latency. The most crucial characteristics in High Performance Computing (HPC) are exceptional processing performance and minimal latency. Grid computing relies on High Performance Computing (HPC) centers. A network of interconnected high-performance computing centers constitutes a vast grid that operates on the basis of service-oriented architectures (SOA), which is a very robust and efficient framework. Data center-based cloud computing is more generally embraced than grid computing. A data center that prioritizes not just great processing performance but also low latency is more well-rounded than a HPC center.

Notional Feature – Service Aligned

The service-adapted approach is akin to, but more pragmatic than, the notion of Service-Oriented Architecture (SOA) in grid computation. Accessibility and abstraction are essential factors in achieving the idea of service orientation. By using virtualization and other advanced knowledges, the fundamental planning is abstracted, while minimizing the amount of information exposed to the user. Cloud user opacity is present. Abstraction decreases the need for cloud users to acquire knowledge about the intricacies of cloud planning and lowers the level of complexity in utilization advancement.

Simultaneously, the fundamental components of the underlying architecture may be easily accessible by the cloud user. Cloud users may quickly use all available resources by examining system factors such as processor power and storage capacity. Cloud computation services are characterized into three main types based on the offered capability: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and SaaS [6, 7]. IaaS refers to the provision of extensive computer properties, including processing power, storage, and system capacity. Using storage as an instance, when a user utilizes the cloud computing storage service, they just pay for the portion they use without purchasing any physical disks or having any knowledge about the data's location that they are working with. Occasionally, the term IaaS is also referred to as Hardware-as-a-Service (HaaS).

Mechanical Feature 1 – Loose Connection

Loose connection is the foundational technological principle of cloud computation and extends beyond the loose connection approach used for utilization relation. By using virtualization or other similar knowledges, the structures are divided into logical or physical components. The performance of one component has little impact on other components. For instance, the platform serves as a conceptual layer that may separate and protect various apps that are operating on it. Primarily, cloud computing operates inside a client-server architecture. Cloud users establish a loose connection with cloud providers or servers. The users possess less data or control reliance. However, data reliance plays a crucial role in high-performance computing (HPC). We can just establish validations:

User sets $Uset_1$, $Uset_2$,..., $Uset_m$ ($m \geq 1$) comprise users. Provider sets $Pset_1$, $Pset_2$,..., $Pset_n$ ($n \geq 1$) comprise providers. ($Uset_i$ $Pset_j$)Set is the description of the user-set Useti loose coupling with provider-set $Pset_j$. The following three properties are displayed: User groups are separate entities: φ ($0 \leq i, j \leq m, i \neq j$) = $Uset_i \cap Uset_j$. Provider groups are separate entities: φ ($0 \leq i, j \leq m, i \neq j$) = $Pset_i \cap Pset_j$. The following sets are independent of the loose connection (cloud user attaches to cloud provider): The set ($Useti_1$,$Psetj_1$) $\cap$ the set ($Useti_2$, $Psetj_2$) = φ. Using Google, Yahoo!, and Bing as a basic example, these providers are search. Users of the search service can be segregated into separate user sets and are not permitted to use three web pages at once (absolute time). $Uset_{Yahoo}$! $\cap Uset_{Bing}$ $\cap Uset_{Google} = \varphi$. The three giants' data centers, which power basic search interfaces, are separate entities. $Pset_{Bing} = \varphi$ PsetGoogle $\cap$ $Pset_{Yahoo}$!. The loose coupling sets are sovereign $Uset_{Yahoo!}$ $Pset_{Yahoo!}$ Set Uset Pset $\cap$ Set $\cap$ Set($Uset_{Bing}$,$Pset_{Bing}$) = φ .

Independent cloud users may bring forth several additional benefits such as statelessness, scalability, and robust fault tolerance. A contrasting illustration is the strong interconnection of HPC systems that prioritize the resolution of scientific issues. Typically, there are several data dependencies or global synchronizations in various iterations that result in significant delays between compute nodes. These systems use high-speed networks such as InfiniBand instead of the more affordable and widely supported industrial standard Ethernet. It is difficult to conceive of investing a significant amount of time to establish a worldwide harmonization in HPC. However, with array computation, the process of synchronizing world data might take numerous hours or even many days.

Mecanical Feature 2 – Strong Fault Acceptance

Parallel computing offers several fault-tolerant methods. At the low-level, there are always particular hardware fault repair techniques in place. At a higher level, many specialized applications are examined using approaches that target algorithms. Conducting a checkpoint is a very efficient approach at the intermediate level. In high-performance parallel computation structures, the time among two failures may be less than the time it takes for a utilization to complete its implementation. For instance, many scientific computing programs may operate for extended periods, often lasting weeks or more. However, it is very uncommon for these apps to encounter several insignificant or critical mistakes over their entire duration. In this situation, the fault tolerant technology becomes crucial. Otherwise, it has a much lower probability of successfully completing computationally intensive activities within the allotted time. In many scientific applications, where even the slightest inaccuracy is unacceptable and repeating the calculation is time-consuming, the whole calculation states are regularly recorded on stable storage. If an error occurs, the algorithm will roll back to a specific checking point.

Retaining the whole situations of cloud computing structures is superfluous. There is little correlation among two connections. The failure of one operation has no impact on the other, and a partial failure of the system will not result in a cascading effect. There are primarily four locations where errors may arise in cloud computing: inside the provider's infrastructure, between different providers, between the provider and the user, and between different users. In the event of a provider failure, the backup or dismissal of the provider will serve as a replacement for the failed component. Stopping and restarting services is a commonly used strategy when services are not being provided promptly or urgently. The inherent loose coupling of providers, such as data centers, makes it very easy to handle these types of problems. In the event of a problem occurring among givers, the giver-across operation will be automatically aborted and returned with an error indication. Readdressing to other givers is a widely applicable technique that includes distributing the workload throughout the whole cloud system. Fortunately, there are a limited number of transactions that are mostly driven by background management and include many providers. It simply has to do background management once a day or even once a week.

Monetary Feature – Business Framework

The business framework is the primary distinguishing feature between cloud and grid computing. Grid computing is mostly sustained by governmental and academic institutions. This factor dictates the essence of grid computing: the motivation for financial gain is not sufficiently compelling. Grid computing is a scientific endeavour focused on the future advancement of data technology. However, cloud calculation is mostly sustained by colossal IT corporations. Their goal include ensuring that all reserves in cloud computation provide a return on investment (ROI) in the near future or outperform market rivals in the long term. Cloud computing encompasses several business concepts, particularly those pertaining to payment methods. Pay-per-use is often the preferred option in many situations. This is almost identical to the notion of utility computation.

The storage, processing, and system capabilities in cloud computing are analogous to utility services such as gas, electricity, and water in society [8]. These efficacy services are accessible 24/7 in contemporary life. Service providers charge users according on their use of these utility services. Cloud users may be classified into two categories: end users and median users. Cloud services serve as the ultimate goal for end users. The end user uses cloud facilities for individual consumption. The typical user utilizes cloud services and effectively provides professional services to others at a reasonable cost. Occasionally, the end user is not directly responsible for the payment of cloud services. As an example, users of online games make payments for a certain game according on the duration of their online presence. Additionally, a portion of the cost is covered to sustain the operation of the cloud system. This method is not transparent to the end user. Typically, the average user directly pays for the cloud services they utilize. They economize by swiftly entering the market. The average user does not need to handle intricate hardware and software, acquire knowledge of tools, or obtain expertise in cloud computing technologies.

User Practice Feature – Ease Use

The user practice, a key aspect of human-computer interaction, plays a vital role in determining the achievement of an application. Array computing offers enhanced user experience compared to its predecessors, such as grid computing. The cloud service serves as a mechanism to ultimately provide a satisfactory experience for cloud users. Cloud users should have convenient access to the valued services. The essence of user experience lies in the attainment of usability. The ease of use is not just modest but also refined. There are three motives, which define why array computation would be easy to use:

Firstly, most cloud providers issue Internet-based borders that are more straightforward compared to alternative application programme interfaces (API). These interfaces provide a level of simplicity and elegance that effectively conceals the underlying business operations. The interfaces may remain unchanged regardless of any changes in business processes. Secondly, the user experience of online apps is thoroughly examined. The user borders are content-agnostic. The creation of a web utilization follows a comprehensive process that may be separated into three steps: user needs examination, purpose design, and programme operation. The top-down approach prioritizes user practice design as the foundation for the overall function design. The components of the user practice are usefulness, usability, value, desirability, findability, credibility, and accessibility [9]. Thirdly, web 2.0 enhances the level of engagement and communication between internet consumers and service providers. The initial purpose of the web was to facilitate the transmission of hypertext. With the quick and extensive advancements in content sophistication, the web is often used as a distant software program. Web 2.0 is considered to be the seamless progression of user interaction and diminishes the distinction among the Internet and software. The growing AJAX technology is transforming online apps and services into software-like entities.

III.SERVICE MODELS

Currently, cloud computing offers a range of services, with the three major ones being Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) (see **Fig. 2**) These are often referred to as the service frameworks of cloud computing.

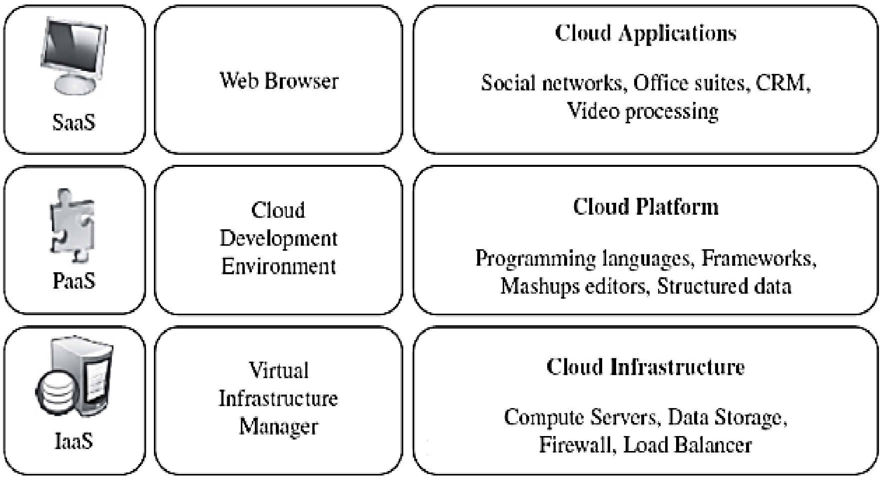

Fig 2. Cloud Computing Service Model.

Infrastructure as a Service

The fundamental computer resources consist of software and hardware elements. They establish the fundamental basis of all computer structure. The IaaS service in cloud computing offers these services to end users of the cloud. IaaS liberates users from the burden of managing these services. Customers have the option to engage any of these services at their preferred level. The user is solely responsible for paying for the use of their resources. Infrastructure as a Service (IaaS) aims to provide operating middleware and computational infrastructure [10]. Grid/Cluster designs provide enterprises high-presentation infrastructures on a rental basis, freeing them from the need to rely on their own properties. Administrations might focus their efforts on production and value issues [11]. The primary principle behind IaaS is the virtualization of resources. The user is able to run their own guest functioning structure on top of the infrastructure offered by the cloud giver. This notion facilitates the autonomous placement of structure that is both dispersed and scalable. The service provider is accountable for the administration, implementation, and maintenance.

Elements of IaaS

The cloud structure comprises many components that are used in the infrastructure service model. Shared resources provide several issues for service providers due to their use by different customers. Several constituents include: Computer hardware, Cloud computing software, Networking and internet connectivity, Service level agreements, Platform virtualization, Utility computing.

Service Level Agreements

Prior to implementing the service-oriented cloud computing`s architecture, clients have a primary worry about the dependability and quality of the services being supplied [12]. The expectations of these services vary across customers, thus, it is necessary to reach a consensus among the consumer and the service offer. The document that outlines the standards and dependability of the service is referred to as a Service Level Agreement. The purpose is to establish, explain, and discuss the terms and states of a contract among a service offer and clients in order to come to a final decision. The QoS characteristic is an integral component of the SLA and must be accurately described. Quality of Service (QoS) encompasses several factors such as reaction time, memory consumption, and throughput, among others [13]. It is crucial to regularly monitor these aspects. This component is crucial since if any term or state is omitted or not addressed, it may cause issues for both users and service givers. SLA encompasses other functionalities such as service measurement, assessment of service conditions, and management services.

Utility Computing

Cloud computing encompasses utility calculation, which encompasses connection bandwidth, calculations, storage, and other related resources. The main aim of utility computation is to reduce the cost of optimization and allocate properties to the end user, charging them a suitable fee based on their utilization. Additionally, it guarantees the effective management of the scalability of cloud infrastructure. The facility provider may improve the structure without interrupting the services, even if the number of users grows.

Cloud Software

Cloud software is employed to seamlessly connect various elements of cloud network and ensure their synchronization. There are several open basis software options accessible on the market, such as Nimbus and Eucalyptus. However, these software solutions are not free from faults and vulnerabilities, which might pose a threat to the cloud structure. In addition, cloud service providers create and employ APIs (Application Programming Interfaces) like HTTP, REST, and SOAP with XML to carry out various tasks, such as access control.

Platform Virtualization
Virtualization is a fundamental process in cloud architecture since it enables the creation of several virtual systems on a single physical system, allowing for the simultaneous execution of different activities. Sharing hardware resources decreases the need for hardware upkeep. By using this approach, it effectively decreases the intricacy and improves the cloud resources scalability.

Internet and Network Connectivity
Cloud organization is geographically spread to decrease latency and mitigate resource harm. The cloud infrastructure components are interconnected by local area networks (LANs) and further linked together using high-speed internet connectivity. The collective components form the whole of the cloud organization.

Computer Hardware
IaaS offers an interface to its clients or users, allowing them to access the dispersed properties of the cloud structure. The resources mentioned include the storage, central processing unit (CPU), and system connectivity elements. These cloud resources need robust security measures, since any vulnerability might jeopardize the whole cloud infrastructure. Any damage or defect in the hardware will lead to service failure.

Software as a Service
SaaS is the maximum level of cloud computation services. SaaS, differs from conventional software services in that it eliminates the requirement for customers to have their own software and hardware elements. With SaaS, users may be autonomous of their own asserts. Users utilize the advanced services accessible by the cloud operator. A prime example of Software as a Service (SaaS) is Google Docs [14, 15]. **Fig. 3** presents various key features of SaaS.

Quality Model
In order to assess and comprehend SaaS, it is necessary to establish a quality model.

Reusability
Reusability is the practice of using software components to develop several applications, and it has significant importance in the cloud computing domain. The core principle of CC is the use of various internet-based services. Specifically, in the case of SaaS, software that can be reused is offered to service customers over the web. The provision of SaaS facilities often establishes one-to-many partnerships. For instance, the number of customers using the services offered by Google Maps, which offers various functionalities for accessing and utilizing shared information both locally and on the map, is significant.

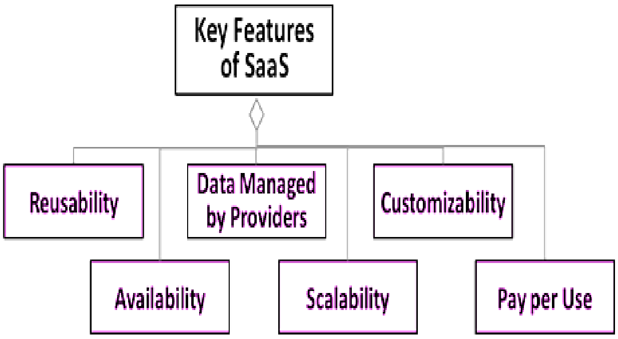

Fig 3. SaaS Quality Model [16].

Data Achieved by Provider
SaaS, is a service that offers users the ability to utilize licensed applications on demand. It is also often used as a software development paradigm. Service providers have the obligation to handle data and set up facilities on their own servers. Therefore, the majority of data generated by users of a service is kept and maintained in data centers by the entities responsible for providing the data. Service clients are not aware of two specific details: the location where their data is kept, and the methods used to manage the data. Therefore, if service providers do not provide reliable functions and data security, clients may question the services and their use may decrease.

Service Customizability
Customizability refers to the capacity of customers to modify services according to their own needs and preferences. Customizability is crucial in order to meet the assorted needs of users. Service benefactors must be able to offer customization options to effectively serve the various requirements of their customers. Internet users may readily use these cloud services and have the potential to become consumers of it. Due to this particular attribute, service providers are unable to adjust their cloud services for many service clients. Service consumers have the ability to effortlessly alter or adjust their services to suit their own requirements. If there is a shortage of customized SaaS service availability, service customers should utilize the services that are available.

Accessibility
Clients may conveniently access SaaS services in Cloud Computing by using a web browser and internet connectivity. The provider's server, responsible for running and deploying SaaS services, does not provide ownership of the SaaS to clients. Therefore, most vendors prioritize achieving optimal service availability. Without the availability of SaaS services, clients are unable to access any feature provided by SaaS. The Gmail service is a prime illustration of this assertion, since it had a total outage on 1 September, 2009 [17]. This resulted in the unavailability of email read and write services for Gmail users. In the cloud computing domain, users have the expectation that SaaS would be available at all times, without any instances of failure originating from a single source [18]. Service should be continuously accessible regardless of maintenance, disappointments, upgrades, or any kind of assault.

Scalability
Scalability is an essential need for cloud computing as it governs the degree of adaptability and agility of a system or application. Additionally, it indicates the growing prevalence of software use. The service provider manages cloud resources, and clients have no authority over the resources consumed by the services. The service provider has the responsibility to enhance resource capacity to satisfy customer requests seamlessly and to ensure continuous communication with the consumer.

Pay Par Use
When using software facilities, it is crucial for users to not have incurred any expenses, since they are the rightful owners of the service. However, it is essential that they remunerate in accordance with the extent of service use. This pertains to the scenario when a client wants to use a service. The consumer will create a link with the cloud and thereafter terminate the usage of the services. Subsequently, he will be responsible for remunerating the period of service use.

Platform as a Service
PaaS offers customers a growth stage to create and manage their apps and cloud-specific tools. An example of PaaS cloud computing may be seen in **Fig. 4** [19]. The PaaS offers an Integrated Development Environment (IDE) that encompasses data protection, a scalable architecture, application hosting, and backup and recovery. PaaS differs from SaaS in that whereas SaaS involves the deployment and development of utilizations, PaaS serves as a platform or foundation for the growth of such applications. Since PaaS offers the development environment and platform, cloud providers are required to provide the necessary infrastructure, development tools, and programming environments.

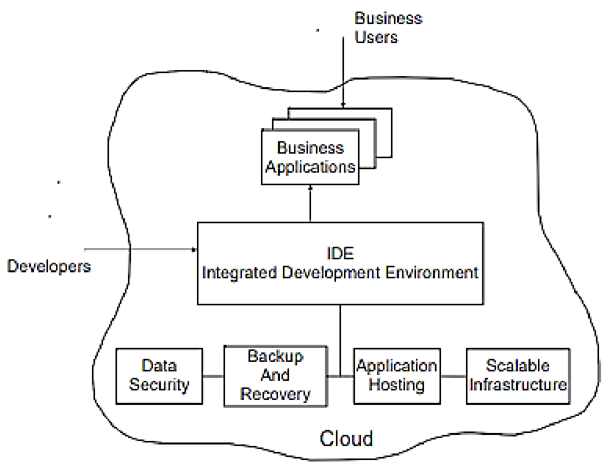

Fig 4. The PaaS Concept.

Stakeholders of PaaS
Based on the use of properties and management of organization, there are three categories of PaaS shareholders [20].

PaaS Hoster
A PaaS hoster is accountable for provisioning the physical infrastructure via IaaS, which is essential for meeting customer requirements [21].

PaaS Provider
A PaaS provider is responsible for furnishing developers with a development platform, enabling them to work on web utilization advancement without requiring expertise in servers and front-end utilizations [22].

PaaS User
The PaaS user is the developer responsible for creating apps. In order to operate on that platform, it is necessary to have a browser-based utility. Customers will be charged based on their use of the services [23].

IV. DEPLOYMENT MODELS

The literature has examined several cloud deployment methods [24]. There are four deployment types listed in reference [25] as follows:

Private Cloud

This approach involves a cloud provider offering cloud infrastructure services to a specific organization that has several users. This structure is intended only for their exclusive use and need. The entity responsible for owning, managing, and operating this cloud infrastructure may consist of the association itself, a third party, or a collaboration between the association and a third party. This private cloud may be located either off-site or on-site.

Community Cloud

This approach involves a cloud provider offering cloud structure to several associations that create a community. This community has a common objective, security needs, compliance considerations, and policies. This infrastructure is intended just for their specific purposes and requirements. The operation, management, and ownership of this cloud may be accredited to either an association, a third party, or a joint collaboration between the association and a third party. The Community cloud may be located either off-site or on-site.

Public Cloud

This framework is distinct from the preceding framework in that it is accessible to the general public; it is not restricted or limited to a certain community. This architecture allows for the provisioning of a public cloud that may be used by the general public to fulfill their requirements. The entity responsible for the ownership, management, and operation of this cloud infrastructure may vary and may include a government, private organization, corporation, or academic institution. It is also possible for many entities to coexist inside a single cloud and receive services from the same benefactor.

Hybrid Cloud

This paradigm consists of two or more placement modes, namely public, private, or communal. The cloud substructure might consist of a mix of these models. An enterprise may integrate its data center, private cloud, and public cloud to access services and data from both sources, resulting in a cohesive and efficiently managed computing environment. A cloud is classified as hybrid when data is transferred between a data center and either a public or a private cloud, or vice versa.

Virtual Private Cloud

A Virtual Private Cloud (VPC) is a secluded computing ecosystem that exists inside a larger public cloud infrastructure. A VPC essentially creates rationally segregated parts inside a public cloud to offer a simulated private ecosystem. Similar to other cloud ecosystems, VPC resources may be accessed instantly to adjust according to requirements and provide extensive customization options. This method is a middle ground among a private and a public framework in terms of cost and functionalities.

Inter-Clouds

Inter-cloud, often known as "cloud of cloud", is a conceptual framework for cloud computation amenities that involves integrating many different clouds into a one entity, allowing for smooth and immediate access to resources as needed. Inter-cloud enables a cloud to access resources outside of its own network by using existing agreements with other cloud providers [26]. **Table 1** displays a comparative analysis of the six cloud deployment models, including several parameters as indicated below [27].

Table 1. Comparative Analysis of Six Deployment Models

	Inter	**Hybrid**	**Community**	**VPC**	**Private**	**Public**
Used by	Any client	Medium accessibility	Depend upon number of cooperatives	Depend on Authorization of the user	Limited people can access	Anyone can access
Size of data center	More than hybrid cloud	Less than private cloud	Public cloud > 15000> Private cloud	50000>TO <80000	Around 50,000s	Around 50,000s
Workload	Extremely flexible or dynamic	Extremely flexible or dynamic	Ideal for managing a heavy workload	Appropriate for managing a heavy task	Unsuitable for managing a heavy task	Regular workload with brief demand peaks
User's control	Full control	Total authority in the private sphere and restriction in the public sphere	High control but limited by community policies	Full control	Full control	Limited control

Managed by	CSP	Establishment and CSP	Numerous companies or CSP	CSP		CSP
Location	On premise	On or off premise	On or off premise	On premise	On or off premise	Off premise
Ownership	CSP	Organization and CSP	Several organizations	CSP	Single organization	CSP
Demand for in-house hardware	No	Though not needed, in-house hardware is ideal	No	No	Though not needed, in-house hardware is ideal	No
Cost	Very Inexpensive	Higher than a public framework, but less exclusive than a private one	Participants split the expenses.	Affordable	Very expensive	Very Inexpensive
Setup flexibility	Very adaptable	Very adaptable	Limited adaptability; settings are typically somewhat predetermined	More than a public cloud, but less than a private one	Very flexible	Very little flexibility; most service providers only give preset configurations
Security and privacy	Very high	Incredibly high because the data is stored on a private cloud	High (if members collaborate on security policies)	Extremely low; inappropriate for sensitive data	Extremely high; perfect for business data	Extremely low; inappropriate for sensitive data
Scalability	High (when properly configured)	High (when properly configured)	Fixed capacity limits scalability	Extremely high because your cloud segment is the only one with tenants.	High because there aren't any additional system occupants	Low, most suppliers only give a small number of resources
Reliability	High (for clients)	High (with the right setup)	Depends on the community	Prone to failures and outages	Exalted (with the appropriate group)	Prone to interruptions and failures
Data control	Exceedingly high (when properly configured)	Exceedingly high (when properly configured)	High (if members collaborate)	Low, all control is with the provider	High because you are the system's owner	Low, all control is with the provider
Ease of use	Easy to use	Challenging to operate if the system was improperly configured	Very simple to utilize since members develop protocols and assist with problem-solving	Easy to use	Intricate and necessitates an internal team	Very easy to use
Ease of Setup	Easy to set up, with the majority of the work done by the supplier	Incredibly difficult to put up because of linked systems	Because of group customs, it is simple to establish	Simple to set up, the majority of the work is done by the provider (unless the client requests otherwise)	Somewhat challenging to put up while your team develops the system	Easy to set up, with the majority of the work done by the supplier
Performance	Excellent	Good	Very good	Low e	Excellent	Low to medium

V. DATA INTEGRITY ISSUES

Data saved in the cloud is susceptible to harm during transmission to and from cloud data storage. Given that the computation and data are delegated to a distant server, it is essential to consistently uphold and authenticate the data`s integrity to ensure that both the computation and data remain unaltered. Data integrity refers to the state of data being protected from any unauthorized alterations or modifications [28]. Any alteration to the data should be noticed. Computation integrity refers to the assurance that program execution proceeds as intended and remains protected from any kind of malware, insider threats, or malevolent users who may attempt to alter the program's execution and produce an inaccurate outcome. Any aberration from standard calculation should be identified. Integrity should be verified both at the information level and the calculation level. Data integrity plays a crucial role in recovering lost data and detecting any instances of data tampering. Here are two instances illustrating potential violations of data integrity.

Manipulation or Data Loss

Users own an extensive amount data (records), which motivates cloud companies to provide SaaS (software-as-a-service). These records may be viewed on a daily basis, which makes its necessary to ensure their accuracy. This need arises due to the inherent characteristics of array computing, where information is stored in a distant cloud that is both insecure and unreliable. Due to the lack of reliability of cloud services, there is a menace of information loss or illegal alteration by those without proper authorization. Data may be intentionally or mistakenly manipulated in several instances. In addition, there are other administrative failures that might result in data loss, such as restoring or obtaining improper backups. The attacker might exploit the users' subcontracted information since they no longer have control over it.

An Untrusted Remote Server Calculating User Behavior

Cloud computing encompasses more than simply data storage. Furthermore, many complex calculations need the use of cloud-based processing capabilities to successfully execute their operations. Consequently, users delegate their calculations to other sources. Given that the cloud benefactor is outside the security border and lacks transparency to the duty owner, there is no means of verifying the integrity of the computation. Occasionally, the cloud provider's behavior may go unnoticed, since it conceals any divergence from the expected execution of computations [29, 30]. Due to the inherent value of the resources to the cloud provider, the job could not be executed effectively. While the cloud provider may be seen as more secure, there are several concerns arising from the cloud provider's fundamental infrastructure, susceptible programming, or mispositioning.

VI. CONCLUSION AND FUTURE SCOPE

This paper discusses the features, service frameworks, and issues related to data safety in cloud computing. By examining the conceptual and technological features, it becomes clear that cloud computing's service-adapted approach and loose coupling design allow for exceptional scalability, efficient resource usage, and easy accessibility for users. The investigation of Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and Platform-as-a-Service (PaaS) frameworks emphasizes the range of options accessible to fulfill different user requirements and preferences, while also emphasizing the fundamental economic motivations for the implementation of cloud technology. Furthermore, the classification of integrity issues demonstrates the relevance of establishing trust in the information and the calculations performed in cloud solutions such as data loss, data tampering, and data theft. As more enterprises employ cloud computing for their computing demands, these difficulties should not be overlooked to safeguard and guarantee the integrity of data. Therefore, for future research, more emphasis should be placed on enhancing the security measures in order to minimize the ways in which the cloud computing technology can be exploited. In addition, this is a clear indication that the industry stakeholders, researchers, and lawmakers require coming up with standardized procedures and regulations on management and protection of data in cloud environments. These challenges must be met and solved to improve cloud computing security and to fully benefit from cloud technologies for all parties and to ensure data availability, integrity, and confidentiality.

CRediT Author Statement

The authors confirm contribution to the paper as follows:
Conceptualization: Aaron Mike Oquaye and John Atta Mills; **Methodology:** Aaron Mike Oquaye and John Atta Mills; **Writing- Original Draft Preparation:** Aaron Mike Oquaye and John Atta Mills; **Visualization:** Aaron Mike Oquaye; **Investigation:** John Atta Mills; **Supervision:** Aaron Mike Oquaye; **Validation:** John Atta Mills; **Writing- Reviewing and Editing:** Aaron Mike Oquaye and John Atta Mills; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

The datasets generated during the current study are available from the corresponding author upon reasonable request.

Conflicts of Interests

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Funding

No funding was received for conducting this research.

Competing Interests
The authors declare no competing interests.

References
[1]. M. G. Avram, “Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective,” Procedia Technology, vol. 12, pp. 529–534, 2014, doi: 10.1016/j.protcy.2013.12.525.
[2]. N. Kaaniche and M. Laurent, “Data security and privacy preservation in cloud storage environments based on cryptographic mechanisms,” Computer Communications, vol. 111, pp. 120–141, Oct. 2017, doi: 10.1016/j.comcom.2017.07.006.
[3]. A. Botta, W. de Donato, V. Persico, and A. Pescapé, “Integration of Cloud computing and Internet of Things: A survey,” Future Generation Computer Systems, vol. 56, pp. 684–700, Mar. 2016, doi: 10.1016/j.future.2015.09.021.
[4]. S. Marston, Z. Li, S. Bandyopadhyay, J. Zhang, and A. Ghalsasi, “Cloud computing — The business perspective,” Decision Support Systems, vol. 51, no. 1, pp. 176–189, Apr. 2011, doi: 10.1016/j.dss.2010.12.006.
[5]. Y. Sun, J. Zhang, Y. Xiong, and G. Zhu, “Data Security and Privacy in Cloud Computing,” International Journal of Distributed Sensor Networks, vol. 10, no. 7, p. 190903, Jul. 2014, doi: 10.1155/2014/190903.
[6]. A. J. Ferrer, D. G. Pérez, and R. S. González, “Multi-cloud Platform-as-a-service Model, Functionalities and Approaches,” Procedia Computer Science, vol. 97, pp. 63–72, 2016, doi: 10.1016/j.procs.2016.08.281.
[7]. W. Tsai, X. Bai, and Y. Huang, “Software-as-a-service (SaaS): perspectives and challenges,” Science China Information Sciences, vol. 57, no. 5, pp. 1–15, Mar. 2014, doi: 10.1007/s11432-013-5050-z.
[8]. R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, “Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility,” Future Generation Computer Systems, vol. 25, no. 6, pp. 599–616, Jun. 2009, doi: 10.1016/j.future.2008.12.001.
[9]. M. Nowakowski, “Analysis and Evaluation of Information Usefulness and User Experience For Content Presentation in Electronic Media,” Procedia Computer Science, vol. 176, pp. 3654–3664, 2020, doi: 10.1016/j.procs.2020.09.021.
[10]. S. S. Manvi and G. Krishna Shyam, “Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey,” Journal of Network and Computer Applications, vol. 41, pp. 424–440, May 2014, doi: 10.1016/j.jnca.2013.10.004.
[11]. A. Ordanini and P. Pasini, “Service co-production and value co-creation: The case for a service-oriented architecture (SOA),” European Management Journal, vol. 26, no. 5, pp. 289–297, Oct. 2008, doi: 10.1016/j.emj.2008.04.005.
[12]. F. Qazi, D. Kwak, F. G. Khan, F. Ali, and S. U. Khan, “Service Level Agreement in cloud computing: Taxonomy, prospects, and challenges,” Internet of Things, vol. 25, p. 101126, Apr. 2024, doi: 10.1016/j.iot.2024.101126.
[13]. M. Haghi Kashani, A. M. Rahmani, and N. Jafari Navimipour, “Quality of service-aware approaches in fog computing,” International Journal of Communication Systems, vol. 33, no. 8, Feb. 2020, doi: 10.1002/dac.4340.
[14]. K. CHEN and W.-M. ZHENG, “Cloud Computing: System Instances and Current Research,” Journal of Software, vol. 20, no. 5, pp. 1337–1348, Mar. 2010, doi: 10.3724/sp.j.1001.2009.03493.
[15]. J. Mineraud, O. Mazhelis, X. Su, and S. Tarkoma, “A gap analysis of Internet-of-Things platforms,” Computer Communications, vol. 89–90, pp. 5–16, Sep. 2016, doi: 10.1016/j.comcom.2016.03.015.
[16]. S. Aleem, F. Ahmed, R. Batool, and A. Khattak, “Empirical Investigation of Key Factors for SaaS Architecture,” IEEE Transactions on Cloud Computing, vol. 9, no. 3, pp. 1037–1049, Jul. 2021, doi: 10.1109/tcc.2019.2906299.
[17]. B. P. Rimal, A. Jukan, D. Katsaros, and Y. Goeleven, “Architectural Requirements for Cloud Computing Systems: An Enterprise Cloud Approach,” Journal of Grid Computing, vol. 9, no. 1, pp. 3–26, Dec. 2010, doi: 10.1007/s10723-010-9171-y.
[18]. X. Zhou, C. Xu, and B. Kimmons, “Detecting tourism destinations using scalable geospatial analysis based on cloud computing platform,” Computers, Environment and Urban Systems, vol. 54, pp. 144–153, Nov. 2015, doi: 10.1016/j.compenvurbsys.2015.07.006.
[19]. N. Bassiliades, M. Symeonidis, P. Gouvas, E. Kontopoulos, G. Meditskos, and I. Vlahavas, “PaaSport semantic model: An ontology for a platform-as-a-service semantically interoperable marketplace,” Data & Knowledge Engineering, vol. 113, pp. 81–115, Jan. 2018, doi: 10.1016/j.datak.2017.11.001.
[20]. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015, doi: 10.1109/comst.2015.2444095.
[21]. D. Villegas et al., “Cloud federation in a layered service model,” Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1330–1344, Sep. 2012, doi: 10.1016/j.jcss.2011.12.017.
[22]. G. Agapito and M. Cannataro, “An Overview on the Challenges and Limitations Using Cloud Computing in Healthcare Corporations,” Big Data and Cognitive Computing, vol. 7, no. 2, p. 68, Apr. 2023, doi: 10.3390/bdcc7020068.
[23]. L. O. Colombo-Mendoza, G. Alor-Hernández, A. Rodríguez-gonzález, and R. Valencia-garcía, “MobiCloUP!: a PaaS for cloud services-based mobile applications,” Automated Software Engineering, vol. 21, no. 3, pp. 391–437, Feb. 2014, doi: 10.1007/s10515-014-0143-5.
[24]. Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief, “A Survey on Mobile Edge Computing: The Communication Perspective,” IEEE Communications Surveys & Tutorials, vol. 19, no. 4, pp. 2322–2358, 2017, doi: 10.1109/comst.2017.2745201.
[25]. Prof. H. B. Patel and Prof. N. Kansara, “Cloud Computing Deployment Models: A Comparative Study,” International Journal of Innovative Research in Computer Science & Technology, vol. 9, no. 2, pp. 45–50, Mar. 2021, doi: 10.21276/ijircst.2021.9.2.8.
[26]. N. Grozev and R. Buyya, “Inter-Cloud architectures and application brokering: taxonomy and survey,” Software: Practice and Experience, vol. 44, no. 3, pp. 369–390, Dec. 2012, doi: 10.1002/spe.2168.
[27]. M. H. Ghahramani, M. Zhou, and C. T. Hon, “Toward cloud computing QoS architecture: analysis of cloud systems and cloud services,” IEEE/CAA Journal of Automatica Sinica, vol. 4, no. 1, pp. 6–18, Jan. 2017, doi: 10.1109/jas.2017.7510313.
[28]. P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, vol. 102, pp. 902–911, Jan. 2020, doi: 10.1016/j.future.2019.09.028.
[29]. I. A. T. Hashem, I. Yaqoob, N. B. Anuar, S. Mokhtar, A. Gani, and S. Ullah Khan, “The rise of ‘big data’ on cloud computing: Review and open research issues,” Information Systems, vol. 47, pp. 98–115, Jan. 2015, doi: 10.1016/j.is.2014.07.006.
[30]. L. M. Vaquero, F. Cuadrado, Y. Elkhatib, J. Bernal-Bernabe, S. N. Srirama, and M. F. Zhani, “Research challenges in nextgen service orchestration,” Future Generation Computer Systems, vol. 90, pp. 20–38, Jan. 2019, doi: 10.1016/j.future.2018.07.039.

ISSN: 3080-7484