Journal of Software Engineering and Applications, 2024, 17, 297-320
https://www.scirp.org/journal/jsea
ISSN Online: 1945-3124
ISSN Print: 1945-3116

Analysis of Secured Cloud Data Storage Model for Information

Emmanuel Nwabueze Ekwonwune[1], Udo Chukwuebuka Chigozie[1], Duroha Austin Ekekwe[2], Georgina Chekwube Nwankwo[3]

[1]Department of Computer Science, Imo State University, Owerri, Nigeria
[2]Department of Computer Science, Gregory University, Abia, Nigeria
[3]Department of Computer Science, Anambra State University, Awka, Nigeria
Email: ekwonwuneemmanuel@yahoo.com

How to cite this paper: Ekwonwune, E.N., Chigozie, U.C., Ekekwe, D.A. and Nwankwo, G.C. (2024) Analysis of Secured Cloud Data Storage Model for Information. *Journal of Software Engineering and Applications*, **17**, 297-320.
https://doi.org/10.4236/jsea.2024.175017

Received: April 3, 2024
Accepted: May 25, 2024
Published: May 28, 2024

Abstract

This paper was motivated by the existing problems of Cloud Data storage in Imo State University, Nigeria such as outsourced data causing the loss of data and misuse of customer information by unauthorized users or hackers, thereby making customer/client data visible and unprotected. Also, this led to enormous risk of the clients/customers due to defective equipment, bugs, faulty servers, and specious actions. The aim if this paper therefore is to analyze a secure model using Unicode Transformation Format (UTF) base 64 algorithms for storage of data in cloud securely. The methodology used was Object Orientated Hypermedia Analysis and Design Methodology (OOHADM) was adopted. Python was used to develop the security model; the role-based access control (RBAC) and multi-factor authentication (MFA) to enhance security Algorithm were integrated into the Information System developed with HTML 5, JavaScript, Cascading Style Sheet (CSS) version 3 and PHP7. This paper also discussed some of the following concepts; Development of Computing in Cloud, Characteristics of computing, Cloud deployment Model, Cloud Service Models, etc. The results showed that the proposed enhanced security model for information systems of cooperate platform handled multiple authorization and authentication menace, that only one login page will direct all login requests of the different modules to one Single Sign On Server (SSOS). This will in turn redirect users to their requested resources/module when authenticated, leveraging on the Geo-location integration for physical location validation. The emergence of this newly developed system will solve the shortcomings of the existing systems and reduce time and resources incurred while using the existing system.

Keywords

Cloud, Data, Information Model, Data Storage, Cloud Computing, Security System Data Encryption

1. Introduction

1.1. Background of the Study

Securing Cloud Data Storage using UTF ((Unicode) Transformation Format) base 64 algorithm. There is increasing attention given to computing in cloud in the academia and commercial environments recently. Many researchers have recognized the potentiality of storage of data in cloud data, which defines Data Storage as a Service (DaaS) concept. However, the tremendous growth of data has also increase desire for many institutions and organizations to put into consideration where to preserved, manage and access data promptly, and how these data could be secured properly. Computing in cloud is recent paradigm resulting from years of scientific research on distributed computing, virtualization, networking, and web software services. It is natural evolution of the widespread adoption of virtualization, service-oriented architecture, autonomic and utility computation [1]. This area of computing is in support of creating new level of applications running on fault resistant hardware devices that include smart phones; mobile devices and tablets or Personal Digital Assistants (PDAs); using cloud storage technology in data storability. This new technology is needed in our institutions as education demand is constantly increasing due to advances and positive change of e-campus solutions.

Furthermore, it is imperative for e-campus systems to meet the recent trend in technology. Education institutions are thrilled at the capability of institutions to take their salient data from management and physical infrastructure and give attention to core competencies of the innovation of storability of data in the cloud. The agility provided by computing in cloud excites institutions the most. However, various institutions of learning, organizations, and individuals, dealing with astronomical data are concerned more on the computing in cloud, is associated security risks, particularly in storage of data, as improperly secured data may make them experience partial loss of control of system that ordinarily they should be highly accountable for. Among the rapidly growing areas of information technology is cloud. Computing in cloud technology offers the ultimate combination of hosting platform and internet storage services Computing in cloud provides scalable and cheap computing infrastructure, which delivers qualitative services when needed, and helps in implementing online applications for quality output. Ultimately, computing in cloud goal is the provision of scalable and cheap computing infrastructure when needed that also delivers high level quality services. It came with internet, which has provided easy access to computing sites that are remote. This frequently uses web-oriented applications or tools, which users have full access to via web browsers which gives the feeling that they have the program installed on remote hosts systems.

The National Institutes of Standards and Technology (NIST) gave more objectives and coherent definition of computing in cloud, as a model that enables convenient, accessibility to configurable pool of computing resources shared on networks inclusively, web servers, storage applications that are readily provided and made available the least effort of management or interactions of providers of web services. Typical providers of computing in cloud deliver applications for business that are common online, and that could be accessed via Web browsers, while storing the software and the data on the server. Many people see computing in cloud as service that is needed in different ways and one in every three persons utilizes it. Many people are continuously transferring data into cloud for its flexibility. It is adjudged to be an application to successfully use in organizations for its application, which allot room for large data storage and easy accessibility to the stored data when required. Due to the increasing level of people storing their important and personal data in cloud, storing the data safely is also becoming a serious concern. Data security under storage is preventing many organizations, multinationals, and institutions from transferring their data that are sensitive to cloud.

> Cloud computing took the world by storm, now recognized as one, if not the most popular technology in the Information Technology (IT) Industries. Day by Day, a wide range of companies and businesses are becoming more habituated to using many applications of cloud computing because of its compensation as-you-use nature, where clients need not to worry about purchasing assets such as hardware, programs, framework etc., as cost is reduced drastically when compared to the traditional model of computing and the ease at which IT infrastructure solution offered [2]. Cloud computing can be termed as providing information technology resources when demanded through the internet. The whole concept of its operation is in the notion that the work done (data and software) on the client side can be transferred to an unseen cluster of resources on the internet [3]. Cloud computing being a virtual environment has its special security threats and these threats are by far different from the threats in physical systems. This has led to companies and businesses refusing to fully adopt moving to cloud computing environment. In this study, these security concerns will be properly examined and improved upon to be able to give those with doubt the trust to fully embrace cloud computing.

Data Security is the protection of data from an unauthorized user, theft or corruption and thereby providing a high security standard to avoid modification and interception of sensitive data in transmission [4]. Securing sensitive data has raised eyebrow in recent time due to massive increase in transfer, research and transaction over the internet (cloud environment). In order to improve on data transmission over the internet securely, different techniques have been revised with sophisticated approaches such as encryption terminologies in cloud [5].

"Data integrity is the maintenance of and the assurance of data accuracy and consistency over its entire life cycle" [6]. Data integrity also make sure that data is kept safe from third party force and the data is always accurate and reliable irrespective of the period of time it has been stored or how regularly the data is being accessed. Every business and organization invests heavily to keep their confidential data from unauthorized modification thereby enforcing different policies to achieve this.

Electronic Business used interchangeably with e-business is define as the overall term that envelops all form that uses of Digital information and communication technology to help and streamline business measures (E-Business, n.d.). With the 24 hour/7 days availability of the internet, and the global exposure and related legal risks associated with the absence of territorial boundaries as well as business hour limitations provide a strong possibility that customers from around the world will visit sites.

Today's technical and legal landscape presents formidable challenges to personal data privacy. First, our increasing reliance on Web services causes personal data to be cached, copied, and archived by third parties, often without our knowledge or control. Second, the disclosure of private data has become common place due to carelessness, theft, or legal actions. Our research seeks to protect the privacy of past, archived data such as copies of emails maintained by an email provider against accidental, malicious, and legal attacks. Specifically, we wish to ensure that all copies of certain data become unreadable after a user-specified time, without any specific action on the part of a user, and even if an attacker obtains both a cached copy of that data and the user's cryptographic keys and passwords.

A Salient concept of data storability is encryption in trusted environment before using cloud storage resource. There are range of encryption algorithms, which have proven secure, which can perform encryption/decryption operations e.g., AES, Serpent and blowfish. Theoretically, algorithms for symmetric key cryptography and asymmetric key cryptography are used for secure data storing in cloud but the latter is slower than the former. However, for performance measurement, symmetric algorithms are preferred. Encryption guarantees confidentiality of stored data and detects any corruption in data.

Major issue of secure storage is management of keys for encryption, because once data is encrypted, keys become the true bits to secure, and if keys are deposited in environment not trusted with data, an intruder can access data and keys to decrypt confidential data. The cryptography method for protecting information is called encryption.

The major debacle to encryption is that data are not hidden, because data encrypted although unreadable still exists, and if hacker is given enough room, he may eventually cryptanalyze the encrypted data. A way out of this debacle, is steganography. Steganography is science and art concealing information into obscure channels to code the information and prevent the anyone from understanding the concealed message; this is the focus of this research.

1.2. Statement of the Problem

Computing in cloud is a trending technology which offers many benefits. As such, most of our institutions and organizations that use large data have decided to transfer important data and objects to cloud and also do online transactions—resource allocations, secure storing of large data from hackers and easy accessibility. Some organizations can boost handling these concerns by moving their businesses to cloud storage providers but for computing in cloud to be widely accepted, security of data in storage remains a sensitive issue that demands some serious urgent considerations, as:

1) Distributed data consequently makes easy physical accessibility to data.

2) Outsourced data can make one loss the control of stored data.

3) The higher people without integrity having access to the stored data, the higher the risk. Cloud storage company will have numerous customers and many servers along with a large team of technical staff having physical and electronic access to virtually data kept in the entire facility.

4) By sharing storage and networks with many other users/customers, the likelihood that some customers may maliciously access other customers data. Sometimes the risk is caused by some erroneous actions, faulty equipment, bugs, and misbehaving servers.

Therefore, security of confidential data from unauthorized access and hackers as many universities and other organizations are susceptible to hackers who can do erroneous damages to the data that are stored in cloud, is a major threat to computing and data storability in the cloud.

Proposing an improved model with efficient security mechanism, to advance on the existing security model that can successfully protect our data domiciled in cloud, is the foundation on which this research is anchored.

1.3. Aim and Objectives of the Study

1) The Aim of this study is to analyze a secure model using Unicode Transformation Format (UTF) base 64 algorithms for storage of data in cloud securely.

The Objectives of Study are:

2) To design an improved secure model for storage of data in cloud using UTF base 64 etc.

3) To develop the secure model using Unicode Transformation Format (UTF) base 64 algorithms for storage of data in cloud securely.

4) To implement the model using programing language C++.

5) To compare proposed model with existing system based on performance analysis.

1.4. Scope of the Study

This study is specifically meant to be deployed in the universities across the country where I am currently carrying out the research. However, the research will be relevant if adopted by many Nigerian tertiary education institutions on completion because this will reduce the risk associated with uploading, storability and irretrievability of data on cloud-based computing infrastructures by the university management.

2. Theoretical Framework

Cloud computing as a channel or route through which computing services such as servers, storage, databases, networking, software, analytics, and intelligence over the Internet ("the cloud") can be accessed or used.

Cloud computing is on-demand access, via the internet, to computing resources—applications, servers (physical servers and virtual servers), data storage, development tools, networking capabilities, and more—hosted at a remote data center managed by a cloud services provider (or CSP).

2.1. Development of Computing in Cloud

Secure data storage is a security concern in computing in cloud which has been discussed. It is a normal concern of any technology and a major key factor when Software-as-a-service (SaaS) users depend on service-providers, for appropriate security [7]. Hence, security concern is the main issue preventing people from fully adopting computing systems in cloud. In cloud, the files are stored in server, hence; accessible at all times: hackers have full time of working hours for cracking the file security walls: encrypting and authenticating the stored information. Computing in cloud is independent on location and servers, which provide on-demand the resources, data, electricity grid and other devices that may be required. It is evolving naturally with widespread virtualization adoption, architecture that is service-oriented coupled with utility computing. Consumers do not have interest for control or expertise of infrastructure technology supporting computation in cloud. The paradigm shift to computation in cloud has been utilized years back in computing community for sign-in networking diagrams as a link to the Internet or components of networks managed outside IT companies' environments. Computing in cloud, however, recently started taking shape. Few people like John McCarthy, the evolutionary computer scientist had suggested in a speech in 1961, that computation in the future would be organized publicly. The idea did not take off then. According to [7] computing in cloud is computing style providing proper link to network and phenomenal amount of computing resources rapidly deployed with great efficacy. Computing in cloud is paradigm for distributed systems that are economy-driven, abstractions, scalable, dynamic, virtualized, managed power of computing, storage, platforms, and services are delivered when needed over the internet to external customers. Computing in cloud is distributed systems composed of dynamically virtualized networked computers as single computing resources arising from service agreements established by negotiation between end users and the IT company providing services in cloud. Cloud deployment models namely public, private, hybrid and community cloud [8] and the four deployment models describe the services the cloud concept of computing offers to customers. NIST equally identified three service models: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (Iaas) are the Service-rendering architectures used often to ascertain services provided in cloud with some abstractions. Furthermore, NIST equally noted in the diagram, important characteristics of computing in cloud [9] and the characteristics are:

1) Self-services on-demand.
2) Broad networks access.
3) Resource pooling.
4) Elasticity rapidity; and
5) Measured services.

Computing in cloud enables suitable network to guarantee a number of resources for computing easily deployable with enormous efficiency to organizations. Figure 1 illustrated the architecture of cloud computing.

Figure 1 shows the terminology of the cloud computing whose functionalities are the interconnection of infrastructure, platform and application. It gathers the necessary Internet Of things (IOT) devices that are interconnected. The diagram above cloud computing application uses either Laptops, Desktops, Phones and Tablets using the Applications going through the content across the platform managing the database using the run time process with available infrastructures.

The infrastructure devices use the platform to manage and run the applications that are installed already in them.

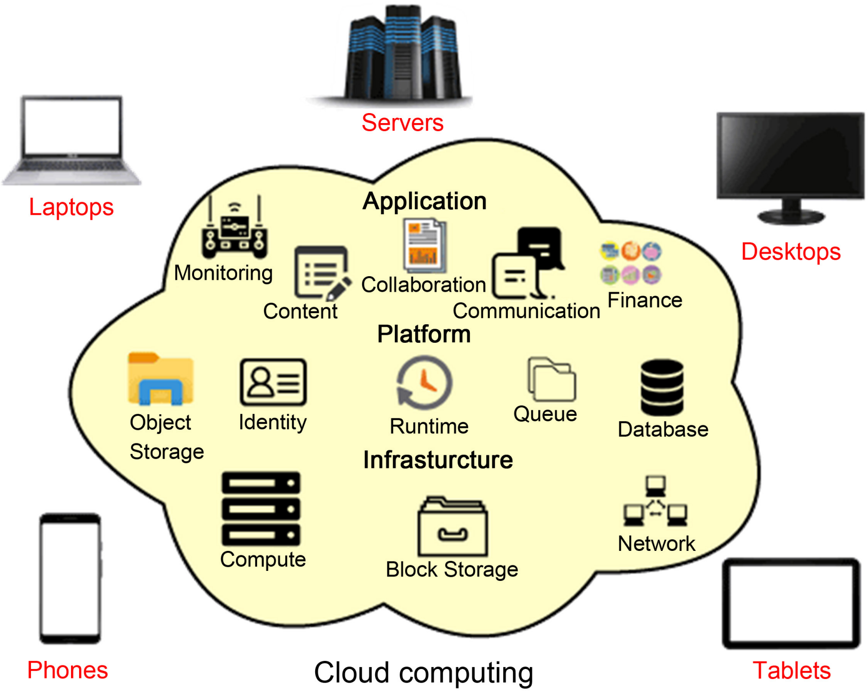

Figure 1. Diagram of computing in cloud (source: Rahul & Nitin, 2023) [10].

2.2. Characteristics of Computing in Cloud

There are five distinct characteristics that are known to be exhibited by computing in cloud [11] [12].

1) Self-Services On-demand. Consumer can provide capabilities for computing, like time for service, and network link needed automatically unilaterally without interaction with the service provider [13]. With cloud computing, you can provision computing services, like server time and network storage, automatically. You won't need to interact with the service provider. Cloud customers can access their cloud accounts through a web self-service portal to view their cloud services, monitor their usage, and provision and de-provision services [13].

2) Access to Network. There are available Capabilities of access to mechanisms that promote multi-client platforms [13]. Another essential cloud computing characteristic is broad network access. You can access cloud services over the network and on portable devices like mobile phones, tablets, laptops, and desktop computers. A public cloud uses the internet; a private cloud uses a local area network. Latency and bandwidth both play a major role in cloud computing and broad network access, as they affect the quality of service [13].

3) Resources Pooling. The providers' resources for computing, serve consumers, and are allocated dynamically, to people who need resources in accordance to consumer's demand [13]. With resource pooling, multiple customers can share physical resources using a multi-tenant model. This model assigns and reassigns physical and virtual resources based on demand. Multi-tenancy allows customers to share the same applications or infrastructure while maintaining privacy and security. Though customers won't know the exact location of their resources, they may be able to specify the location at a higher level of abstraction, such as a country, state, or data center. Memory, processing, and bandwidth are among the resources that customers can pool [13].

4) Elasticity Rapidity. Capabilities can be rapidly and elastically provided automatically, to quickly scale and released to consumers [13]. Cloud services can be elastically provisioned and released, sometimes automatically, so customers can scale quickly based on demand. The capabilities available for provisioning are practically unlimited. Customers can engage with these capabilities at any time in any quantity. Customers can also scale cloud use, capacity, and cost without extra contracts or fees. With rapid elasticity, you won't need to buy computer hardware. Instead, can use the cloud provider's cloud computing resources [13].

5) Measured Service. Systems in cloud control and optimize resources use by leveraging capability abstractly to appropriate the service [13]. In cloud systems, a metering capability optimizes resource usage at a level of abstraction appropriate to the type of service. For example, you can use a measured service for storage, processing, bandwidth, and users. Payment is based on actual consumption by the customer via a pay-for-what-you-use model. Monitoring, controlling, and reporting resource use creates a transparent experience for both consumers and providers of the service.

Figure 2 shows the characteristics of computing in cloud that are essential (source: Tinankoria, 2018) [12].

Figure 2 shows the terminology of the cloud computing whose functionalities of essential characteristics leading from resource pooling, broad network access to measure services or on-demand self-service and rapid elasticity. This is said to be essential due to its ability coordinate the cloud processed. Essential characteristics of cloud computing is the central base that coordinate the whole system sending to On-Deman self-service using automatic provision and to Rapid Elasticity source which is used in measured services to monitor, control, report and bill to control the could application depending on the network accessible by the devices or the resources pooling using the multi-tenancy model using the location independence.

2.3. Cloud Deployments Model

There are four distinct cloud deployment models, and this classification came about from the exact hosting the cloud and they include public, community, private, and hybrid cloud [1] [10].

Private cloud

1) Community cloud;

2) Public cloud;

3) Hybrid cloud.

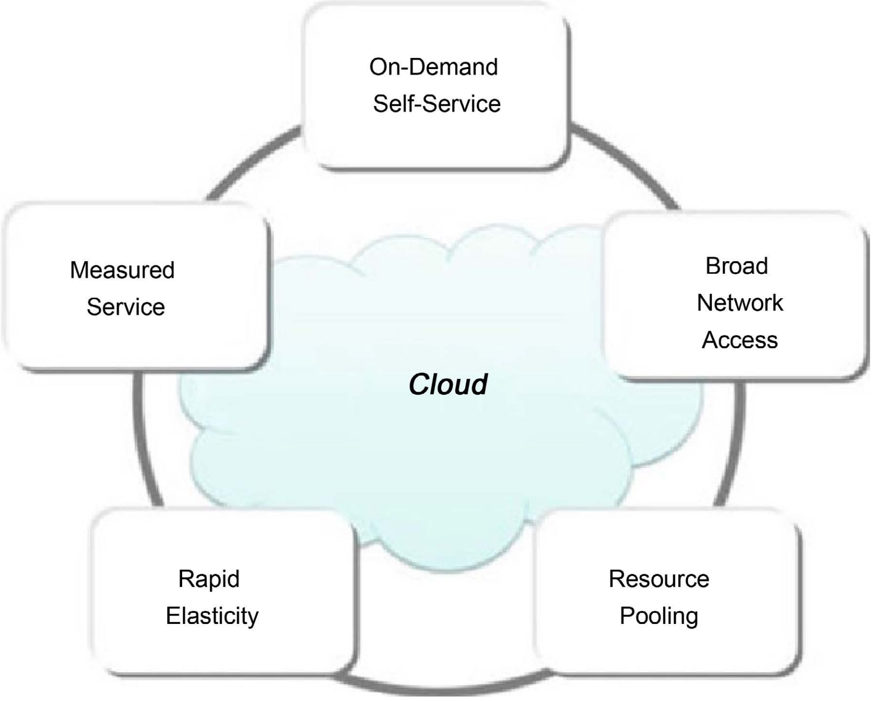

Figure 2. Characteristics of computing in cloud that are essential (source: Tinankoria, 2018) [12].

Cloud for Private is data centers of organizations. Management of a company owned Cloud controls how applications execute on the infrastructure, the place where they run, and the people or organizations using it—has control over the infrastructure. Private cloud often called Internal Cloud; is distinct and secured environment, accessed and operated by only specified clientele. It permits authorized users access only and gives the organization greater and direct data control. This model is like the traditional model used by enterprise before now but with advantages of virtualization. A Private Cloud relies on the virtualization organizations existing infrastructure. Private cloud examples according to [14], are:

1) Eucalyptus;
2) Ubuntu Enterprises Cloud;
3) Amazon Private Cloud;
4) VMware Infrastructure in Cloud;
5) Microsoft's Data center.

Figure 3 above shows a private cloud that can only be accessed by the client(s) who are within the private security perimeters. The clients that are blocked from accessing the private cloud are those that don't have the subscribed access or that doesn't have the right to access the date only the client with legitimate access path can access or subscribed to the private cloud.

On-site private cloud uses private cloud to manage the subscriber with the security perimeter by the clients accessing the private cloud within the security perimeter. The blocked access stops access from the private cloud.

Figure 4 shows only the access from boundary controller of the clients that can access private cloud within the security perimeters while un wanted clients are still been blocked from accessing the private cloud. The diagram above the cloud providers facility and subscriber facility.

The cloud providers facility is a private cloud provider that controls the inside and outside of boundary controller which manage the block access control. The subscriber's facility manage the clients accessing the private cloud from the within the security perimeter or controlled the subscriber-controlled security perimeter.

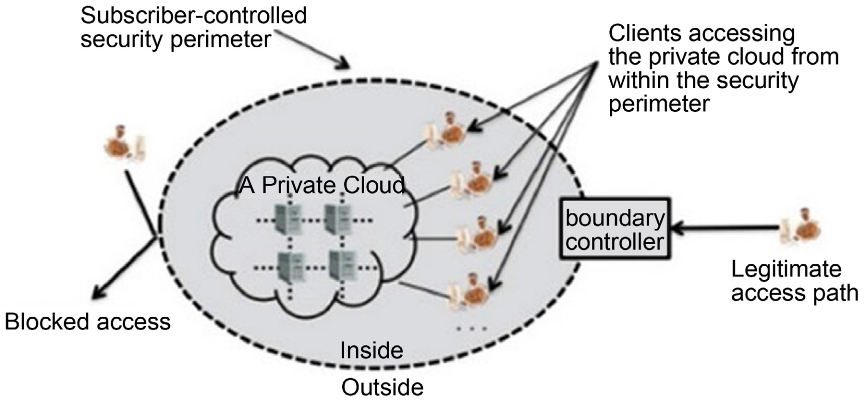
Subscriber-controlled security perimeter
Clients accessing the private cloud from within the security perimeter
A Private Cloud
boundary controller
Legitimate access path
Blocked access
Inside
Outside

Figure 3. On-Site private cloud (Source: Narayana, 2018) [11].

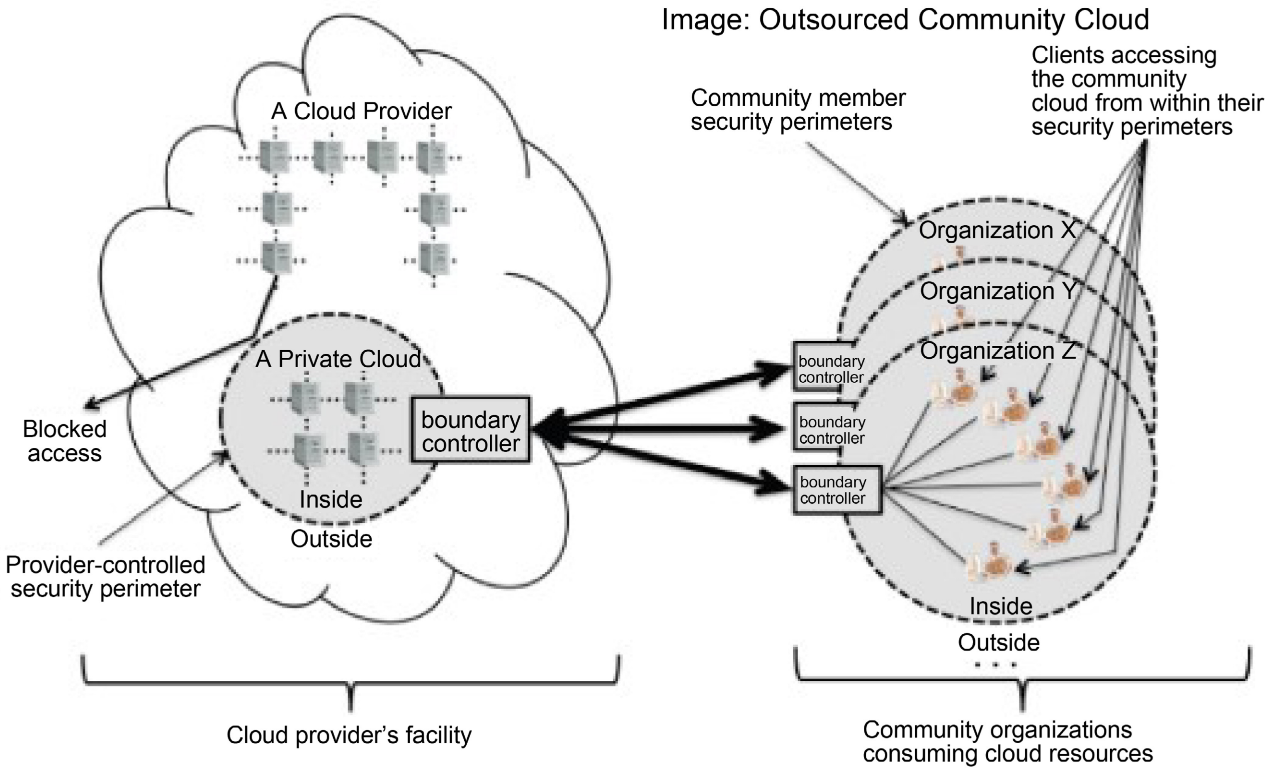
Image: Outsourced Community Cloud
A Cloud Provider
A Private Cloud
boundary controller
Inside
Outside
Blocked access
Provider-controlled security perimeter
Community member security perimeters
Clients accessing the community cloud from within their security perimeters
Organization X
Organization Y
Organization Z
boundary controller
boundary controller
boundary controller
Inside
Outside
Cloud provider's facility
Community organizations consuming cloud resources

Figure 4. Private cloud outsourced (Source: Narayana, 2018) [11].

1) Community Cloud

This model offers cloud infrastructures shared by organizations and it supports specific community, security requirements, mission, policy, and compliance considerations. Government departments, universities, central banks etc find model applicable [15]. Community cloud also has two possible scenarios [15]. *On-site Community Cloud Scenario Applies to community clouds implemented on the premises of the customers composing a community* [15].

Outsourced Community Cloud is clouds are applied to communities' cloud, which are hosted by a company.

Community Clouds include:

a) Google Apps for Government (Big data)

b) Microsoft Government Community Cloud (MGCC).

Figure 5 shows community cloud where only the community members within security perimeters are allowed to access the community cloud. Only those within their security perimeter remotely can have the access to the community cloud as members of the community. This community member that are blocked from accessing the cloud is because they don't have the right pat or access code. Organization A, B, and C access only data from the local cloud using the inner security perimeter and exchange boundary with the organization X, Y, and Z using the client accessing the community cloud from within their security perimeters.

Figure 6 diagram shows community cloud are outsourced only the

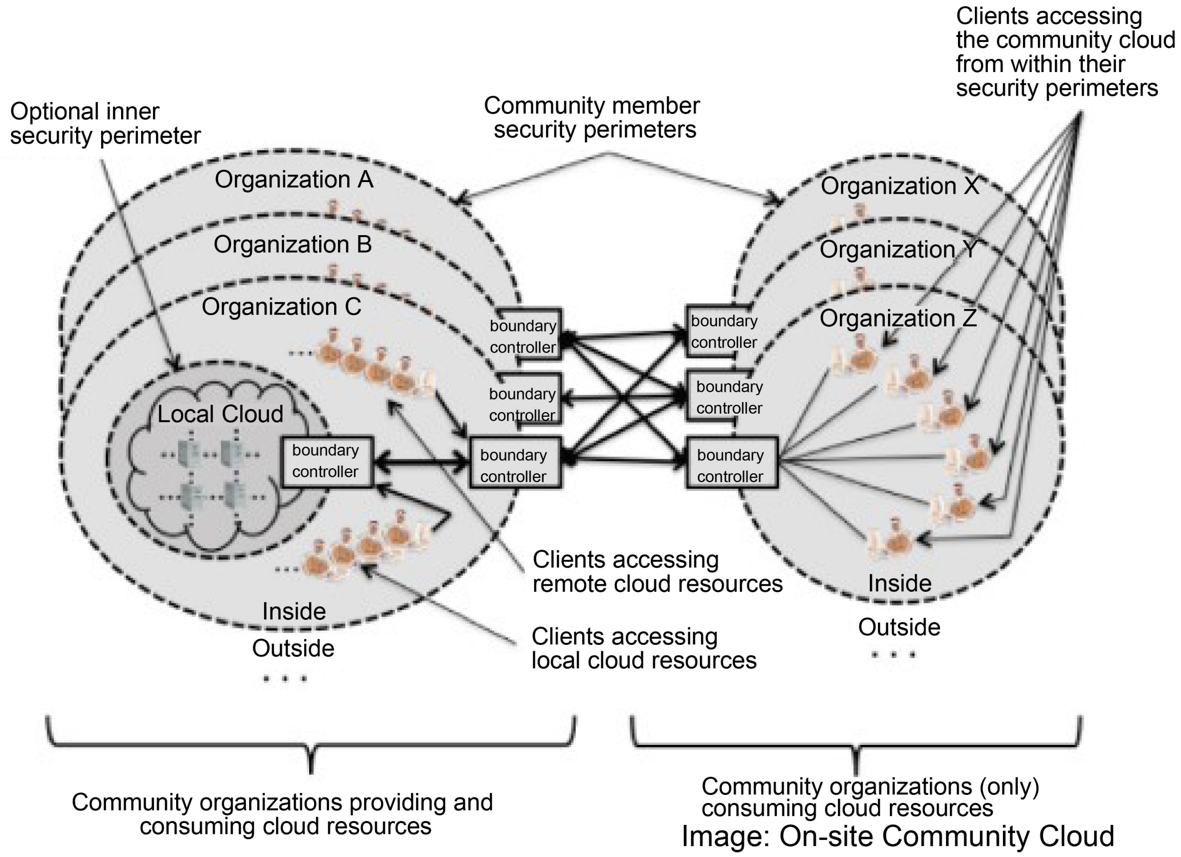
Clients accessing the community cloud from within their security perimeters
Optional inner security perimeter
Community member security perimeters
Organization A
Organization B
Organization C
Organization X
Organization Y
Organization Z
Local Cloud
boundary controller
boundary controller
boundary controller
boundary controller
boundary controller
boundary controller
boundary controller
Clients accessing remote cloud resources
Clients accessing local cloud resources
Inside
Outside
Inside
Outside
Community organizations providing and consuming cloud resources
Community organizations (only) consuming cloud resources
Image: On-site Community Cloud

Figure 5. On-Site community cloud (Source: Narayana, 2018) [11].

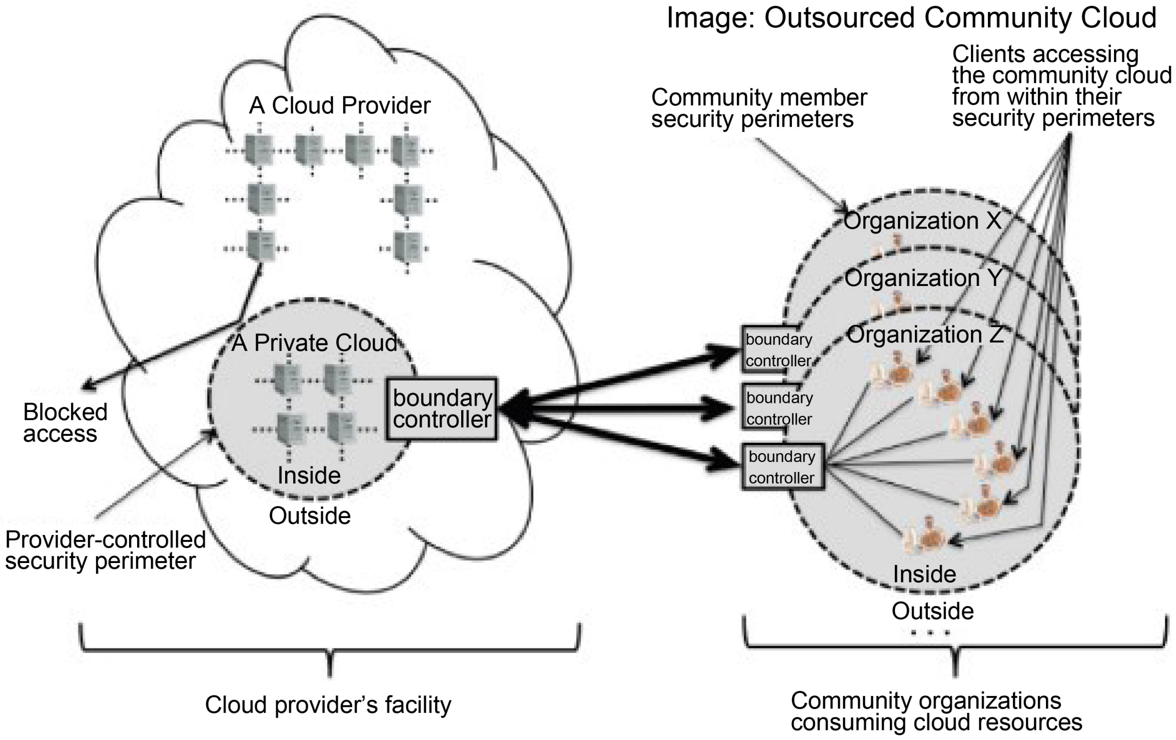
Image: Outsourced Community Cloud
A Cloud Provider
Community member security perimeters
Clients accessing the community cloud from within their security perimeters
Organization X
Organization Y
Organization Z
A Private Cloud
boundary controller
boundary controller
boundary controller
boundary controller
Blocked access
Inside
Outside
Provider-controlled security perimeter
Inside
Outside
Cloud provider's facility
Community organizations consuming cloud resources

Figure 6. Outsourced community cloud (Source: Narayana, 2018) [11]..

community members security perimeters are allowed to access the community cloud. Only those within their security perimeter remotely can have the access to the community cloud even though its outsourced loud account as members of the community. These community members that are blocked from accessing the cloud is because they don't have the right pat or access code.

2) Public Cloud

This model is common. This cloud is accessible by the public. Its ownership belongs to the providers of cloud services. Public cloud also allows the hosting at the vendors premises as seen in Figure 7. The customers have no location visibility of computing in cloud but organizations use resources in cloud. Public clouds include:

a) Googles Application Engine;

b) Microsoft Windows Azure;

c) IBMs Smart-Cloud;

d) Amazon EC2.

3) Hybrid Cloud

This is decomposition of cloud culminating into an entity that is unique bounded together by technology that are standardized, which ensures data and applications portability bursting in load-balancing in-between clouds. Hybrid Cloud may involve usage of hardware physically along with virtualized cloud server instances together to provide one common service [16]. Hybrid cloud examples:

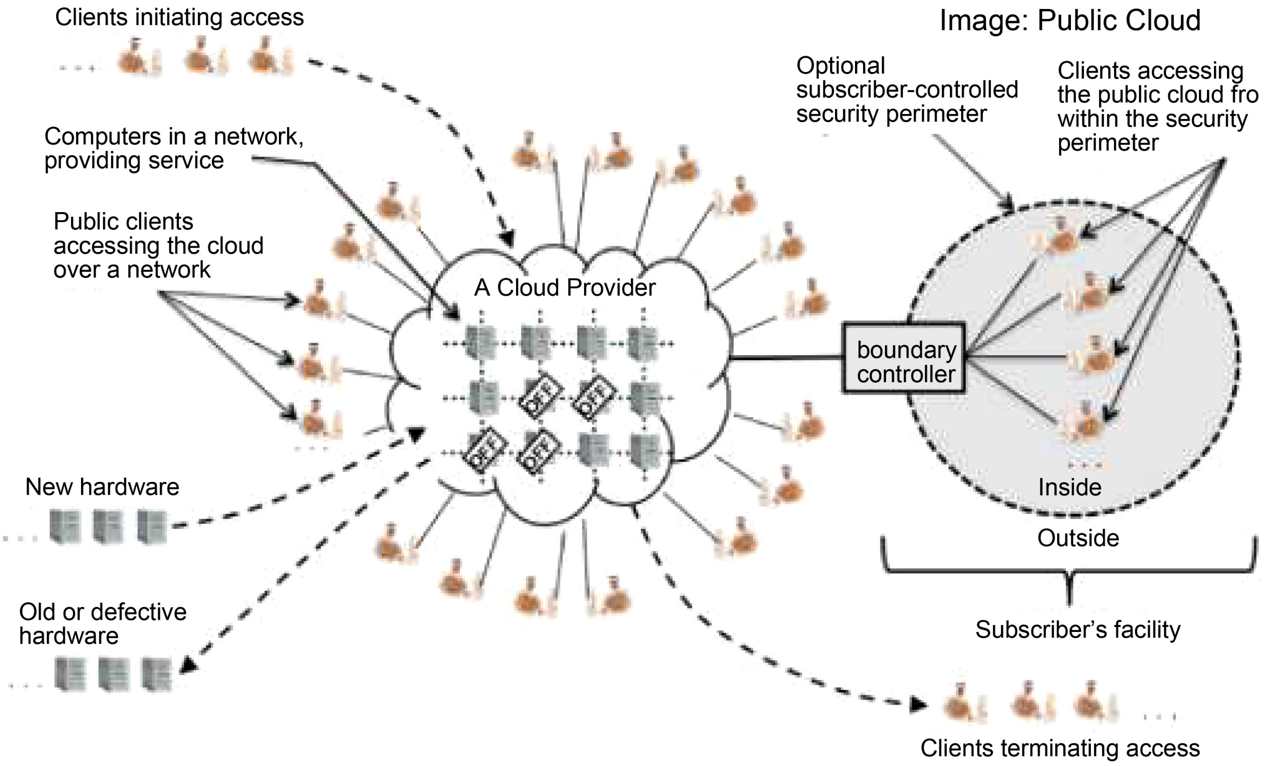
Clients initiating access
Image: Public Cloud
Optional subscriber-controlled security perimeter
Clients accessing the public cloud fro within the security perimeter
Computers in a network, providing service
Public clients accessing the cloud over a network
A Cloud Provider
boundary controller
Inside
Outside
Subscriber's facility
New hardware
Old or defective hardware
Clients terminating access

Figure 7. Public cloud (Source: Narayana, 2018) [11].

a) Windows Azure

b) VM wares Cloud (Hybrid Cloud Services)

Figure 8 shows hybrid cloud system. Hybrid cloud system is the cloud system that consists of the on-site private cloud, outsource private cloud, on-site community cloud, outsource community cloud and all communicate with the public cloud. All cloud system interchanges and communicate with each other cloud system working seamlessly.

3. Cloud Deployment Implications

Any organization opting for cloud usage irrespective of the cloud deployment model to be used must addressed the following implications [17]. Network Dependency: Regardless of the network choosing from but the network must be reliable to ensure good performance. Need for IT skills: this ensures proper management of devices of users' access in cloud, resources, etc. Also, these IT staff or users must be well updated in recent skills for the cloud environment.

1) **Multi-tenancy Risk**: This particular risk has been limited by private cloud on-site which gives access to particular clienteles thereby restricting possible attackers and subscribers from organizations. This risk is higher if single server gives room for workload emanating from subscribers. As such the security risk increases the susceptibility to attackers, with this assessment, public cloud risky from multi-tenancy perspective.

2) **Data Import/Export and Performance Limitations**: It is of important to note that the on-demand big data importing or exporting is scarcely limited by the network of cloud capacity. This particular issue is limited but not in totality by provisioning high-performance and/or high-reliability networking within the subscriber's infrastructure.

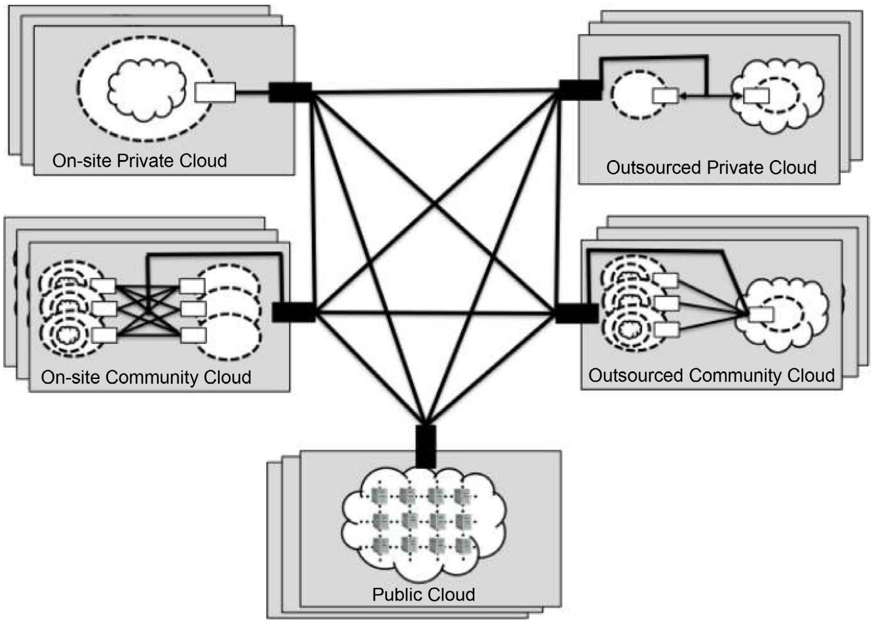

Figure 8. Hybrid cloud (Source: Narayana, 2018) [11].

Workloads Locations-Efficient hardware resources management is workloads definition.

3.1. Cloud Service Models

The cloud service models are Infrastructures-as-a-Service (IaaS), Platforms as a Service (PaaS), and Software as a Service (SaaS) as identified by [18] [19] [20] [21].

1) Infrastructure as a Service (IaaS): This model provides resources like servers, storage and networks in the form of virtualized systems on Internet. Resources are provided and managed in fairly chunky units-whole (physical or virtual) servers, storage pools etc. generally unaware of what applications are running on them [22]. The Infrastructures as a Service (IaaS). This is computing infrastructural resource at reduced ownership cost.

This model gives opportunity to users to run any software while having control absolutely of allocated resources management [23]. With IaaS, cloud users tp better control security in comparison with other model once security is not bridged on the monitor of virtual machines [24]. IAAS model allows its subscribers take charge of virtual machines (*i.e.* a customer can choose operating system of interest for each dedicated virtual machine).

Its Application

IaaS is the most flexible cloud model that helps manage and customize your IT hardware infrastructure according to your requirements. IaaS gives you access to all the essential computing resources including storage, computing, and networking, without purchasing them [25].

2) Software as a Services (SaaS): This model provides services applications whenever needed like software for conferencing, email, and business applications like ERP, CRM, and SCM [26]. Examples include online word processing, and spreadsheet tools, CRM services and web content delivery service [27] application is used by client without having control on operating systems, hardware, network infrastructure for running the application. The SaaS is much at times free, easy access with good consumer adoption and proven business model. Major weakness of SaaS, is, users are solely based on application design and purpose without exhibiting any control or any idea how the computing technology works.

Its Application

SaaS is the ideal choice for small businesses and start-up that do not have the necessary budget and resources to deploy on-premise hardware. Saas applications have simplified remote collaboration, transferring of content, and scheduling visual meetings in a pandemic-affected world.

3) Platforms as a Service (PaaS): This model enhances [28] Customers simply use hosting environments for running their applications and they have some control over environment of applications but having no control on hardware or operating network infrastructure. The model simply provides platforms for applications design frameworks. This service providers, provides virtual machines, abstract hardware and operating systems controlled via API. Examples include: Amazons E-C2, and S3, Terremark Enterprise Cloud, Windows Live cloud; Skydrive and Rackspace. Platforms as a Service (PaaS); means by which operating systems can actually be rented online. The services model let customers to rent servers (virtualized) and associated.

Its Application

PaaS is a great choice if your project involves multiple developers and vendors. PaaS solutions are specific to applications and software development and typically include Cloud infrastructure, middleware software, and user interface.

Figure 9 above shows Cloud Computing Models consist of three services namely Software as a Service (SAAS), Platform as a Services (PAAS), and Infrastructure as a Services (IAAS).

1) Software as a Service: is the part of the Cloud Computing Models that consist of the Business process, industrial Application etc.

2) Platform as a Service: is the Model that consists of the services controlling development tool, database connections, web application and runtime.

3) Infrastructure as a Service: is the part of the Model control or manages the servers, Networking, Data center fabric and its storage.

The Models service interchanges all services with each other, the infrastructure hosts the platform and software runs on the platform.

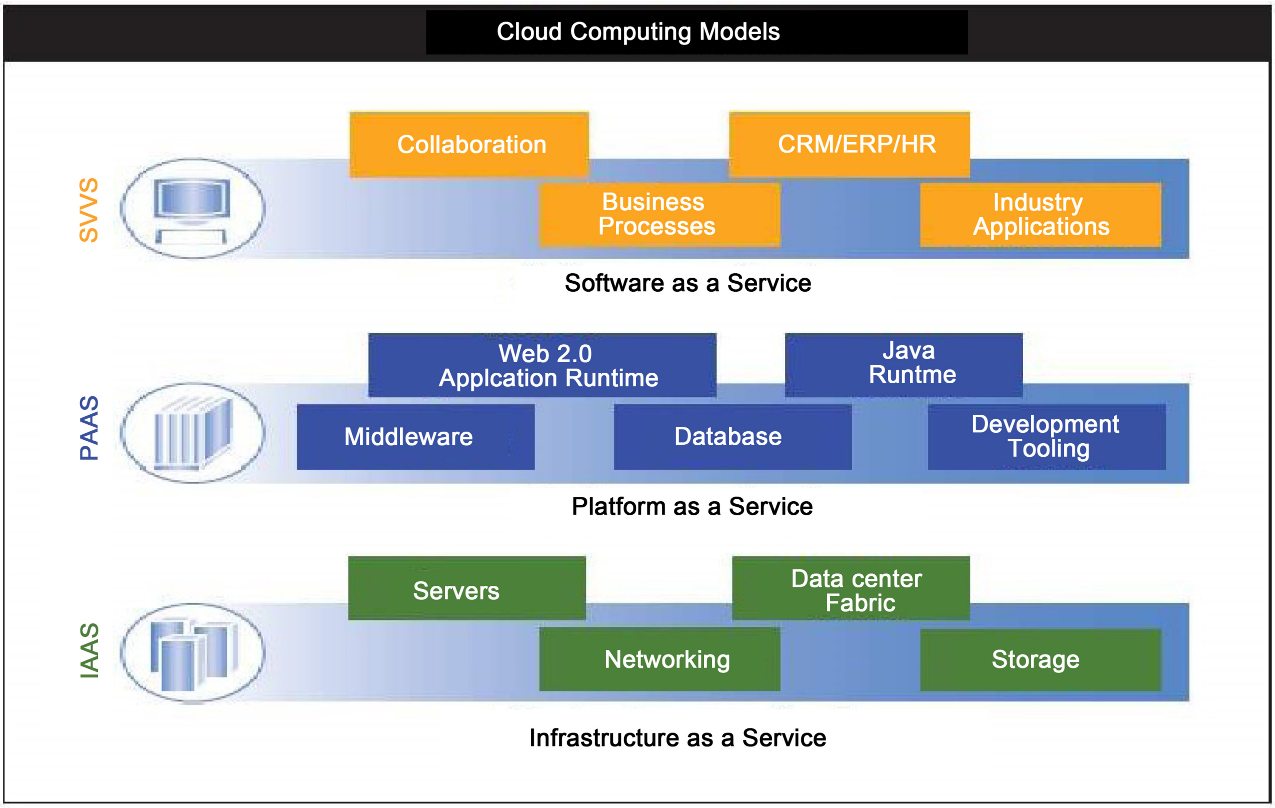

Figure 9. Models for computing in cloud (source: Pranita and Ubale, 2023) [29].

3.2. Data Storage in Cloud

Storage in cloud is virtualized storage on demand and formally called data Storages as-a Services (DaaS). This is delivery on network of compatible virtual storage of data services, depending on request for a service.

Expansion of data and keeping it preserved will definitely make any institution or organizations and institutions to integrate management of data and usage, from creation to end [20]. identified that data storage in cloud provides the opportunity to store sensitive data online into cloud maintained by the service provider. Data storage in cloud offers large storage available for use, with three significant attributes: access via Web services APIs on non-persistent network connections [30] availability of storage, and pay on usage [20]. Storage services like Microsoft Azure and Amazons S3 adequately provide cloud services with dynamic storage. Therefore, Security, Reliability and data availability in storage becomes the major concern of every cloud service user. Storage in cloud therefore is model of storage, which store digital and logical data. The physical storage spans multiple servers, and the physical environment is typically managed and owned by the hosting company.

Providers of data in cloud have the onus of protecting data, and the environment is physically protected. People and organizations lease or buy from the service providers storage capacity to store user, organization, or application data. Data storage in cloud uses Applications having Programming-Interface (API) like utilization storage system of cloud. The commonest of these kinds are REST although there are others, which are based on SOAP (All these APIs are known for establishing internet service requests [20].

3.3. Architecture for Data Storage in Cloud

Data Storage in cloud initially refers to hosted object storage but relatively, the term is broadened to mean storage of data as service. Data Storage in cloud is highly virtualized infrastructure computing in cloud having accessible interfaces, near-instant elasticity and scalability, multi-tenancy, and metered resources. Different providers for storage of data in cloud use different architecture to show their platform for storage of data in cloud. But the diagram in figure depicts the generalized architecture of cloud storage system consisting components mainly three in number [31].

1) **Cloud Interface Layer**: This layer is provided by the providers of cloud to connect users cloud storage to services of cloud online. This layer applies authentication and authorization techniques to authenticate the users.

2) **Data Managements Layer**: This layer is used for distinct cloud client data management. This particular layer handles things as data storage, content distribution across storage location, data partitioning, synchronization, maintaining consistency, replication, controlling movement of data over network, backup, data recovery, handling millions of users, maintaining metadata, catalogue, etc [32].

3) Storage Layer: This layer is virtualization and basic storage section.

Virtualization: Storage virtualization gives illusion of unified storage. It maps distributed heterogeneous storage devices continuous storage space and creates a shared dynamic platform. It is implemented by storage virtualization technology. Few virtualization technologies provide built-in, security, availability and scalability to applications.

4) Basic Storage: It comprises of database servers and storage-devices of heterogeneous nature [32] like Direct Access storage (DAS), Storages Area Network (SAN), Network Attached Storage-NAS [33].

Figure 10 above shows the cloud user access through the user internet by subscribing from cloud client interface who owns cloud account either direct or reseller to data management layer for distribution, backup, data read/write. This can be done passing the storage virtualization oath before the cloud user could gain access to the cloud data storage either from cloud of Network Access storage or Storge Access Network.

From the above cloud architectural diagram; it shows that the cloud user 1, 2, 3, 4 etc can access the client interface 1and n via the Internet (WAN) to retrieve data from the storage device either Network Access storage (NAS) or Storage Access Network (SAN). The figure is divided into three layers 1. Cloud Interface layer, Data Management layer and Storage layer.

3.4. Issues of Storing Data in Cloud

Several issues identified when companies, organizations or educational sectors move their application or data in clouds. Computing in cloud allows these applications and data to resident in storage providers in cloud whose management is yet to be fully trusted and secured. As such the following issues listed below shall be discussed in other to understand the underlying issues in using cloud

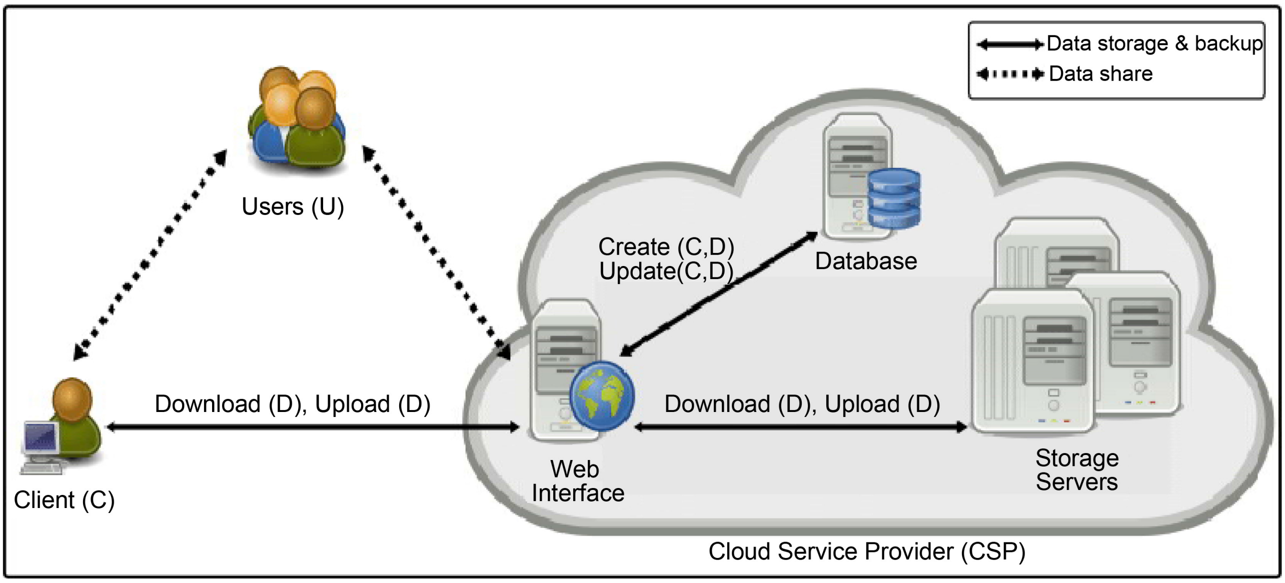

Figure 10. Cloud storage architecture.

storage services [34]. The underlying fact remains that traditional computing, computing in cloud makes use of the technology of virtual computing. In that case, there is every tendency that user data and their personal details are scattered instead of being in a particular physical location or center of virtual data even outside the border of the users nationality. Data privacy protection will face the controversy of different legal systems. Users may trade information when in cloud [35]. Depending on task, users analyze critical computing task is done from attackers' perspective. Privacy issues are;

i) Trust which identifies if there is an unauthorized users of information.

ii) Uncertainty as regards proper data destruction by one who controls data retentiveness, occurrence of breaches and how the fault is determined.

iii) Compliance addresses difficulty in trans-borders data flow requirements.

1) Security

Security is a reason why organizations and institutions of higher learning not leveraging the other underlying benefits cloudy computing. Security of cloud is inclusive in areas like storage security, computation security, network security etc. The security risk considerations are; storage of data externally, public internet dependence, zero control, multi-tenancy and internal security integration [19]. Providers of services in cloud, use encryption mechanisms for data storing and transmission, user's authentication and authorization. The worry of most clients is remote data susceptibility to hackers on the cloud. The sensitivity of service providers of cloud on the afore-mentioned is very high hence they allocate reasonable resources to forestall attack.

2) Trust

Trust concern against security and privacy is also serious because of involvement of third party. For example, in April 2022, Amazons Elastic Compute Cloud service crashed during a system upgrade, knocking customers websites off-line all over for several hours for several days. Another incident happened on the same month. The braking into the PlayStation of Sony by hackers which exposed 77 million people personal information created doubt about cloud privacy, security and these eroded users trust in cloud [36].

3) Ownership

According to [37] once data taken to the cloud, users normally have control loss fears, while the providers have the fear of not protecting customer's right. In other to solve this issue of loss of rights concern cloud providers draft well-skilled agreements that is user-sided which enables users seek legal representation.

4) Availability and Performance

Applications and data in cloud are available whenever needed by users will help address business organizations worries as per acceptable performance and local system used in accessing servers.

5) Viability in Long Term

Users are assured of the continuous validity of their stored data in computing in cloud provider gets lost or a big company acquires them. Users should ask their potential providers of cloud how they would get users data in a form user can import in replacement applications [20].

6) Data Backup

Users normally get disturbed about being in charge of their plans since cloud providers normally engage in processes of data backup routinely. Recently, many providers give room to customers to dump their data into media and also enabling the customers back up frequently through downloads.

7) Data Conversion and Portability

Switching with services providers is a greatest concern to users in cloud. Difficulty of data transferring, converting it or porting depends on providers of cloud storage format of retrieval of data particularly where format is not disclosed. With time, establishment of standards in computing in cloud will address the issue. Worst case, payment will be required by subscribers for the conversion of their customized data areas of computing in cloud need improvement.

8) Inadequate Data Storage Professionals: Organizations require storage of huge digital data. Storage professionals are required to design, and manage the changing storage requirements. Companies do not have skilled data storing professionals due to lack of data storing technology education.

9) Availability of Limited Funds: Economic slowdown, grant cuts or subsidy removal etc gave rise to companies' consideration of cloud storage as a cheaper alternative to maintenance of system and IT staff.

10) Virtualization: Is the fulcrum of computing in cloud and cloud storage, is virtualization, enables multiple applications on virtual machines in physical server. It is used for delivering greater availability, scalability along with optimization of resources.

3.5. Data Classification

Classification is a form of data analysis that extracts models describing important data classes. Such models, called classifiers, predict categorical (discrete, unordered) class labels. Data classification is a two-step process, consisting of a *learning step* (where a classification model is constructed) and a *classification step* (where the model is used to predict class labels for given data) [38] as shown in **Figure 11**.

In the first step, a classifier is built describing a predetermined set of data classes or concepts. This is the learning step (or training phase), where a classification algorithm builds the classifier by analyzing or "learning from" a training set made up of database tuples and their associated class labels. A tuple, X, is represented by an n-dimensional attribute vector, $X = (x_1, x_2, \cdots, x_n)$, depicting n measurements made on the tuple from n database attributes, respectively, A_1, A_2, $\cdots$, An. Each attribute represents a "feature" of X. Hence the terms feature vector and attribute vector are used interchangeably. Each tuple, X, is assumed to belong to a predefined class as determined by another database attribute called the class label attribute. The class label attribute is discrete-valued and

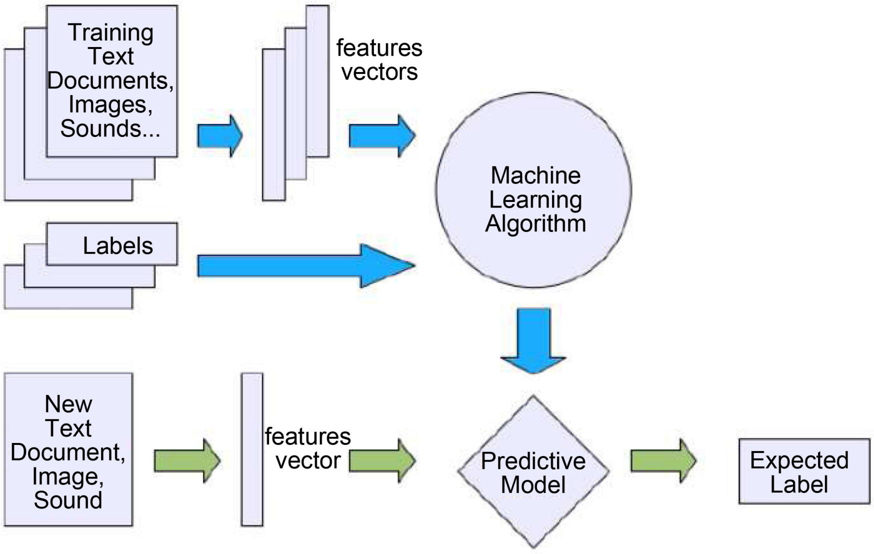
Training Text Documents, Images, Sounds...
features vectors
Labels
Machine Learning Algorithm
New Text Document, Image, Sound
features vector
Predictive Model
Expected Label

Figure 11. A simplified diagram of the general model building procedure for pattern Classification (Source: Kilany, 2013) [39].

unordered. It is *categorical* (or nominal) in that each value serves as a category or class. The individual tuples making up the training set are referred to as training tuples and are randomly sampled from the database under analysis. In the context of classification, data tuples can be referred to as *samples*, *examples*, *instances*, *data points*, or *object* [38]. The learning model will be used then to help predict the outcome in the next step.

In the second step, the model is used for classification. The algorithm is given a set of non-classified data set (unknown), called prediction set, which contains the same set of attributes, except for the prediction attribute that is not yet known. The algorithm then uses the learning model built before to analyze the test set and produces a prediction. The prediction accuracy defines how "good" the algorithm is. The question that rises here is how can we measure the accuracy of the algorithm if the test set is unknown? An answer to this question is to use a

4. Conclusion and Recommendations

In the growing times of Technology, Cloud Computing is a trending technology that offers many benefits. In conclusion, a secure model using Unicode Transformation Format (UTF) 64 algorithms for storage of data would be secured in cloud. Various universities would have the privilege of using this model to carry out widespread research in their different area of study. It would be beneficial to other tertiary institutions because it would diminish the risk related with uploading, storage, and irretrievability of data on cloud-based computing infrastructures. Once the model is compared with the poor data storage and management already existing, it would contract cost that ensues from the university administration, for maintaining and updating the existing websites because the cloud managers will take up that responsibility. The new model will also reduce expenses on purchasing significant software and hardware by the institution, as it is relatively inexpensive, less stressful, reliable, dependable, and will not consume time. Cloud Computing method of storing Data is a better substitute for the normal day-to-day storage devices. Tertiary institutions such as mine should quickly adopt the newest Model of Cloud Computing as their storage uniqueness.

Conflicts of Interest

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

References

[1] Nikita, G. and Toshi, S. (2018) Cloud Computing—SPI Framework, Deployment Models, Challenges. *International Journal of Emerging Technology and Advanced Engineering*, **4**, 19-25.

[2] Ara, R., Rahim, A., Roy, S. and Prodhan, D.U.K. (2020) Cloud Computing: Architecture, Services, Deployment Models, Storage, Benefits and Challenges. *International Journal of Trend in Scientific Research and Development*, **4**, 837-842.

[3] Ajoudanian, S. and Ahmadi, M.R. (2022) A Novel Data Security Model for Cloud Computing. *International Journal of Engineering and Technology*, **4**, 326-329. https://doi.org/10.7763/IJET.2012.V4.375

[4] What Is Data Security? Definition, Solutions and How to Secure Data. https://www.ibm.com/topics/data-security

[5] Singh, K. (2022) Efficiency and Security of Data with Symmetric Encryption Algorithm. *International Journal of Advance Research in Computer Science and Software Engineering*, **2**, 1-9.

[6] Data Integrity (2021). Wikipedia. https://en.wikipedia.org/w/index.php?title=Data_integrity&oldid=1009067843

[7] Heyong, W., Wu, W. and Feng-Kwei, W. (2022) Enterprise Cloud Service Architectures. *Information Technology and Management*, **13**, 445-454. https://link.springer.com/article/10.1007/s10799-032-0139-4

[8] Chakradhara, C.R., Mogasala, L. and Kumar, Y.R. (2020) Cloud: Computing Services and Deployment Models. *International Journal of Engineering and Computer Science*, **2**, 12.

[9] Vadym, M. and Artem, V. (2021) Security Risk Analysis for Cloud Computing Systems. *The 6th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, Vol. 3, Czech Republic, 15-17 September 2011, 340-347.

[10] Rahul, B. and Nitin, C. (2023) Cloud Computing: Service Models, Types, Database, and Issues. *International Journal of Advanced Research in Computer Science and Software Engineering Research*, **3**, 605-701.

[11] Narayana, K.E., Sailesh, K. and Jayashree, K. (2019) A Review on Different Types of Deployment Models in Cloud Computing. *International Journal of Innovative Research in Computer and Communication Engineering*, **5**, 1475-1481.

[12] Tinankoria, D. and Babak, B.R. (2018) Cloud Computing: A review of the Concepts and Deployment Models. *International Journal of Information Technology and*

Computer Science, **6**, 50-68. https://doi.org/10.5815/ijitcs.2017.06.07

[13] Mohammed, U. (2019) A Survey on Authentication in Cloud Computing for Data Storage Security. *International Journal of Advanced Research*, *Ideas*, *and Innovations in Technology*, **3**, 118-121.

[14] Kingson, J. (2018) What Is a Cloud Computing Framework? Benefits and More. https://www.knowledgehut.com/blog/cloud-computing/cloud-computing-frameworks

[15] Mohanakrishnan, R. (2021) What Is Community Cloud? Definition, Architecture, Examples, and Best Practices. https://www.spiceworks.com/tech/cloud/articles/what-is-community-cloud/

[16] Chakradhara, C.R., Mogasala, L. and Kumar, Y.R. (2018) Cloud: Computing Services and Deployment Models. *International Journal of Engineering and Computer Science*, **2**, 3389-3392.

[17] NIST (2011) Cloud Deployment Implications. *International Journal Computer Science*, **2**, 134-140.

[18] Merino (2019) Cloud Service Models. *Journal of Computer Engineering*, **1**, 38-45.

[19] Hashizume, *et al.* (2020) Information Technology and Computer Science. *Journal of Internet Services and Applications*, **2**, 120-128.

[20] Arokia, P.R. and Shanmugapriyaa, R.S. (2022) Evolution of Cloud Storage as Cloud Computing Infrastructure Service. *Journal of Computer Engineering*, **1**, 38-45. https://doi.org/10.9790/0661-0113845

[21] Rountree, D. and Castrillo, I. (2014) Cloud Service Models. https://www.sciencedirect.com/science/article/pii/B9780124059320000049

[22] Eric and Bob (2020) Infrastructure as a Service (IaaS). 33-35.

[23] Dahbur, K., Mohammad, B. and Tarakji, A.B. (2021) A Survey of Risks, Threats and Vulnerabilities in Cloud Computing. *Proceedings of International Conference on Intelligent Semantic Web Services and Applications*, Amman, April 2011, 1-6.

[24] Subashini, S. and Kavitha, V. (2021) A Survey on Security Issues in Service Delivery.

[25] https://www.fingent.com/blog/cloud-service-models-saas-iaas-paas-choose-the-right-one-for-your-business/

[26] Ju, J., Wang, Y., Fu, J., Wu, J. and Lin, Z. (2020) Research on Key Technology in SaaS. *International Conference on Intelligent Computing and Cognitive Informatics*, Washington, DC, 384-387.

[27] ENISA (2019) CRM Services and Web Content Delivery Service.

[28] Mohammed, B.E. (2022) Deployment of Cloud-Based Applications Excluding Software Layers and Hardware Buying and Maintenance Cost.

[29] Pranita, P.K. and Ubale, E.V.S. (2023) Cloud Computing Security Issues.

[30] Shital, A. (2018) Data Storage Access via Web Services APIs on Non-Persistent Network Connections.

[31] https://issuu.com/ijiras/docs/paper_3_1cfc4f054b8358

[32] https://www.scribd.com/document/170495769/IJETTCS-2018-08-24-111

[33] Devenie, C. (2018) Different Types of Storage for Different Problems. https://www.ibm.com/support/pages/different-types-storage-different-problems

[34] Arockiam, L. and Monikandan, S. (2019) Data Security and Privacy in Cloud Staorage Using Hybrid Symmetric Encryption Algorithm. *International Journal of Advanced Research in Computer and Communication Engineering*, **2**, 3064-3070.

[35] Siani (2022) Data Privacy Protection.

[36] Apalina, *et al*. (2018) Issues of Cloud Computing in Regards to Trust.

[37] Mohit, M. and Rajeev, B. (2019) Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing. *IJCSI International Journal of Computer Science Issues*, **10**, 367-370.

[38] Han, J., *et al*. (2012) Data Classification. *International Journal of Advanced Research in Computer and Communication Engineering*, 10-18. https://www.researchgate.net/publication/301078184_Classification

[39] Kilany (2013) Pattern Classification for General Model Building Procedure.