Research Article

INTERNATIONAL JOURNAL OF ENGINEERING BUSINESS MANAGEMENT

International Journal of Engineering Business Management
Volume 14: 1–17

DOI: 10.1177/18479790221093992
journals.sagepub.com/home/enb
SAGE

Adoption of cloud computing as innovation in the organization

Lewis Golightly[1], Victor Chang[2], Qianwen Ariel Xu[1], Xianghua Gao[1], and Ben SC Liu[3]

Abstract

Over the years, there has been a heavy reliance on cloud computing as IT has innovated through time. In recent times cloud computing has grown monumentally. Many organizations rely on this technology to perform their business as usual and use it as a backbone of their companies' IT infrastructure. This paper investigates the organizational adaptation for cloud computing technology - reviewing case studies from various institutions and companies worldwide to provide a detailed analysis of innovative techniques with cloud computing. We investigate the features and delivery approaches cloud computing offers and the potential challenges and constraints we face when adopting cloud computing into the business setting. We also explore the cybersecurity elements associated with cloud computing, focusing on intrusion detection and prevention and understanding how that can be applied in the cloud. Finally, we investigate the future research directions for cloud computing and expand this paper into further articles with experiments and results.

Keywords

Cloud computing, Organizational adoption, Innovation, Technology, Cybersecurity

Date received: 11 February 2022; accepted: 25 March 2022

Introduction

Cloud Computing makes data processing more efficient on multiple computing and storage systems where accessibility is executed through the internet. With the new inventive and innovative computing techniques, the strategies have advanced, supporting the database and network systems that work within the whole internet system. Another new computing approach is known as Grid Computing which was developed in the 1990s - later in 2005, and there was the invention of cloud computing and utility computing.

Virtualization is a crucial aspect of the services and facilities in cloud computing technology, which offers and aggregates numerous standalone virtual computing components into a single hardware platform-CPU, network, storage, and memory. A technology known as a hypervisor (Virtualbox and VMware) is implemented and applied, which is responsible for isolating the virtual machines known as 'VM's'. Hence, the direct accessibility of other virtual disks or virtual machines' memory and applications in the same environment can be prevented by employing this technique. Besides, the presence of hardware abstraction allows enabling, which can help scale computing resources cost-effectively, utilize physical computing platforms and hide their control complexities. Using virtualization technology provides important qualities for cloud computing

[1]Cybersecurity, Information Systems and AI Research Group, School of Computing, Engineering and Digital Technologies, Teesside University, Middlesbrough, UK
[2]Department of Operations and Information Management, Aston Business School, Aston University, Birmingham, UK
[3]School of Business, Quinnipiac University, Hamden, CT, USA

Corresponding author:
Victor Chang, Department of Operations and Information Management, Aston Business School, Aston University, Aston Road, Birmingham B4 7ET, UK.
Email: victorchang.research@gmail.com

environments, including scalability and multi-tenancy occurring in a single software application that can simultaneously serve several users. These qualities are fundamental to cloud computing by enhancing the pooling and sharing of resources to improve many things such as enhanced business value, flexibility, agility, and reduced costs.

The act of provisioning is a fundamental mechanism to distribute assets owned by cloud providers to customers based on cloud virtualization. Cloud providers should generate many virtual machines appropriately and reserve the appropriate resources to maintain users' requirements. The process is completed in three ways: advanced provisioning, dynamic provisioning, and user self-provisioning. Dynamic provisioning provides cloud services and resources - this is often faced with many challenges such as the ideal or optimum configuration for VMs and shortcomings in the technology of disks, CPUs, memory, and network bandwidth to be shared among users. Certain challenges can be present with the practical aspects of virtualization with networking, cloud system configuration and scaling in virtual machines. Cloud resource providers can offer security to virtualization mechanisms by having the ability to eliminate vulnerabilities, attacks, and threats by having the necessary financial, knowledge, and capability aspects (Table 1).

Deploying cloud computing technologies

There are four main technologies that can be used to create and deploy a strategic and meaningful solution to an organization's infrastructure (as highlighted in Table 2). Adoption of these technologies can be observed in businesses throughout recent academic literature. In the work of Tavbulatova, Z.K et al., 2020 where the authors explore the different methods of cloud deployment.[1] The paper firstly focuses on the advantages and disadvantages of utilizing these systems. They begin with Private Cloud, which has benefits such as high protection and Storage capacity, improved data transfer speed, scalability of the organizational resources, and easy-to-use payment systems to significantly reduce energy and maintenance costs of a private cloud system. However, constraints include the need to invest in hardware and licensed software, administrative costs, and the risk of physical threats for data. They then move on to explore the deployment of Public Clouds, which are simple to use and efficient, can deal with an unlimited quantity of computing resources, high data security at the physical and software levels using large data centers, fast and simple implementation of the new information system. The only requirement is internet access, and it presents lower hardware and software costs. In contrast, constraints using this technology include the inability to control the cloud in the organization, dependency on the service provider, and complete dependence on the internet. Hybrid Cloud can maintain data security, reduce costs by transferring resources to cloud providers, and develop a Community Cloud to provide data available anywhere in the world and have low cost for data utilization. However, it does have a high cost for cloud deployment and has a low level of data protection with limited volume.

Case studies in the industry for cloud computing adoption

In the work of Wang, L.C et al., 2021, the authors explore a framework for Cloud Computing deployment for a case study around a scheduling and planning system.[2] The proposed Cloud-APS System consists of four main factors such as: ***(1) User Layer*** - Providing a UI for Users, which

Table 1. Security characterization and explanations.

Security characterization	Explanation
Integrity	This is the assurance of data remaining accurate and unmodified from the original state.
Confidentiality	This is the assurance that user information is kept private from unauthorized personnel to have access.
Availability	This assurance of data reliability is readily accessible to the authorized personnel upon request.

Table 2. Definition of cloud computing.

Cloud technology	Definition
Private cloud	Deployed and managed within a single organization.
Public cloud	Deployed and managed in a third-party organization.
Hybrid cloud	Combination of the private and public cloud technologies.
Community cloud	Sharing computing resources within multiple organizations and has the management operations completed by an in-house IT department or third party.

includes the production planners who planned a production schedule. ***(2) Application Layer*** - This includes the system's application functions, including order adding, order management, intelligent scheduling, schedule query, and MRP updating. ***(3) Service Layer*** - containing the schedule models simulation-based scheduling engine to generate the production and operations schedule based on the parameters. Finally, ***(4) Resource Layer*** - consists of virtual resources, including data and information stored in MES and ERP. Furthermore, in the work of Liu, Z et al., 2022, the researchers investigate the architectural design and implementation of a digital platform for industry 4.0 (known as DIGICOR).[3] With the objective of dynamically forming supply-chain collaborations to pool production capacities and capabilities to address complex supply-chain requests. They propose three main contributions in the research, including The architecture and design and its installation as a platform supporting dynamic modeling of systems and services. The architecture adds to EDSOA mechanisms for modular and efficient communication through semantically defined messages and ensuring compliance with case-specific governance rules procedures for knowledge protection and security. The system contains an array of components for specification such as Company Node, Collaboration Node, Factory node, Tools, Tool Store, Marketplace, DIGICOR portal, DIGICOR gateway, and supporting services. The literature review can be used for a variety of organization adoption methods for existing or future infrastructure and systems.

Review of intrusion detection and prevention

Aldwairi et al. explore how the expansion of the internet has developed into an interconnectivity world.[4] It has also turned networked systems that present to be vulnerable as a target to malicious cyber-attacks coming from any place. These intrusions typically start with an offensive actor discovering the infrastructure, searching for a vulnerable target, and then escalating to further malicious activity towards the target environment. As the attack progresses, more sophisticated techniques are usually applied. Butun et al. describe advanced techniques for attackers utilizing distributed attack bases and obfuscating their network identifications.[5] Therefore, countermeasures, IDS included, require increasingly sophisticated approaches. For example, Handa et al. consider a machine-learning approach to develop an intrusion detection and prevention system used for wireless sensor networks on the internet of things (IoT).[6] While many machine-learning solutions are computationally expensive, and they propose an anomalous intrusion detective protocol (AIDP) utilizing a small attack and fault detection system. The protocol works in three stages: learning, trading, and refreshing. The experience values change depending on the cautions (TAFDS) in the learning stage. Every hub sends its experience esteems to its neighbors in the trading stage. Finally, in the refreshing stage, the standing is refreshing depending on the expertise esteems and trust is refreshing considering the new standing. Further work has been produced by H. Gupta and S. Sharma.[7] where they investigated the security challenges in adopting IoT for smart networks. These authors highlight different attack methods using a layered approach: the first layer is the 'Perception Layer', which includes physical damage, jamming, and malicious code injection. The 'Network Layer' includes traffic analysis, flooding, spoofing and router attacks. The 'Application layer' includes malware attacks, code injection and social engineering, and finally, the 'Multi-Layer Attacks' include DDoS, spyware and cryptanalytic attacks. Further work by Khraisat et al. presents a software-defined network-assisted intrusion detection system.[8] The intrusion detection system they ran is Snort, and multiple concurrent Snort processes run on the same infrastructure. It works by forwarding the potentially malicious data into the SDN controller, which moves data to certain places of an SDN for analysis. The SDN device performs through a docker container on the GNS3 VM, which deals with the connection of different hosts within the SDN.

Huang et al.[9] investigate the current state-of-the-art and future challenges with the protocols used for intrusion detection and prevention systems in wireless sensor networks integrated into the Internet of Things deployment. Their research examines the many security requirements of wireless sensor networks and IoT, focusing on key security properties including Authentication, Integrity, Confidentiality, Non-repudiation, Authorization, Freshness, Availability, Forward Secrecy and Backwards Secrecy. Moreover, they consider common security attacks in Wireless Sensor networks and IoT-based communication. They use a layered approach for defining attacks and the study looks at the requirements of deploying an Intrusion Detection System to mitigate threats in this environment, including successful, careful, and strategic deployment. The overall system should be reliable, producing fewer false negatives and false positives. Hence, the system should not cause harm and expose other vectors of attack. It should also have an economical deployment, not using more network and system resources.

Cirnu et al. examine the current intrusion detection and prevention processes in service-oriented vehicular networks.[10] They start by considering common attacks associated with service-oriented networks: Sybil attacks, DoS attacks, and False alerts generation attacks. They evaluate various intrusion detection agents and propose a scheme for each vehicle to activate an intrusion detection agent to monitor its neighbors. To mitigate against common attacks,

Table 3. Comparison of cloud services.

	Business cloud	Education cloud	Individual cloud
Functions	The business cloud is primarily about handling more extensive or complex data and exchanging data in real-time. Employees can work from anywhere, and managers can view project progress in real-time. Data can be backed up at any time to ensure data security.	The Education cloud is primarily reflected in constructing new learning platforms and tools for distance learning and virtual laboratories. Students can view the latest learning materials at any time via the internet.	Individual cloud is primarily used in the following areas: For students to learn about cloud server operation and maintenance, build personal websites, private cloud storage space, private game servers and deploy private big data services.
Cloud technology	Hybrid cloud	Public cloud	Private cloud
Pros	1. Increase working productivity. 2. Access to data anywhere and anytime, making it easier to work online. 3. Automatic data backup. 4. Cloud server types can be selected according to business content.	1. Saving in IT maintenance costs. 2. More efficient collaboration for students and teachers. 3. Access to resources on any device easily. 4. Scalable. As the number of students grows, increase cloud server performance at any time. 5. Reduced printing of learning materials, more environmentally friendly.	1. Enhance the programming skill ability of users. 2. Individual cloud has higher security and privacy protection than in the public cloud. 3. Have greater control over cloud servers. 4. Deploy personal websites and private databases. 5. Small companies can temporarily use the private cloud for testing, development, and other functions.
Cons	1. Need for high-speed internet support if there is too much data. 2. Core technology limitations if using the public cloud. 3. Increased maintenance costs if using a private cloud. 4. Business cloud servers are expensive.	1. Over-reliance on the internet. 2. Single provider of cloud solutions. 3. Potential security vulnerabilities. 4. Cumbersome data migration to cloud at the beginning.	1. Users manage and deploy cloud services by themselves. 2. Costly and requires a lot of effort to repair if problems occur. 3. Cannot fully meet security regulations for data usage in various countries and regions.

they propose a Rule-Based Intrusion Detection Technique that can defend against common attacks such as Sybil and DoS attacks.

Comparison between cloud computing and grid computing

Grid computing is a term that describes a structure or fabric made up of classified resources. This method is employed to split and outsource hardware equipment and software segments to a significant number of model users. Grid computing could be used in a variety of institutions. Grid computing resources include networks, software licenses, remote devices, printers, memory disk spaces, scanners, cycle processors, etc. The difference between Grid computing and Cloud computing is that the latter has a single ownership. According to Zissis,[11] Grid computing users are obligated to make their hardware and software available to others on a timetable established by grid managers. Cloud computing and grid computing are comparable in many ways. Both approaches gather together disparate computing resources and share their scaling capabilities to execute one or more complicated tasks that are difficult to accomplish with a single resource. The grid computing model is most useful for academic and scientific objectives as it processes computationally complex jobs quicker and cheaply (Table 3).

Clients are required to submit a thorough proposal outlining the research project description and the resources needed so that customers can negotiate with suppliers on the usage of grid resources. Grid computing's major purpose is to increase idle computing capacity user exploitation when tasks cannot be completed remotely.

Tripathi states that Grid computing and cloud computing are distinct in that grid computing is not dependent on a protocol that utilizes their computing resources in lieu of those of other users in the event of a necessity.[12] On the other hand, cloud computing is concerned with commercial enterprises in which suppliers provide offers to the public for usage at an affordable price; the aim is to replace

companies that are unwilling or unable to manage their computing development and management.

Yangui et al. point the main purpose of cloud computing is to segment the material into different parts and deliver them to consumers according to their preferences and interests.[13] From a technical point of view, grid computing refers to the process of integrating resources from several institutions to create a similar pool of computing capabilities that cannot be performed with a single cloud computing structure. These institutions can be dispersed in terms of geography and have the right to control the users of their computing resources.

Grid computing is often implemented using grid middleware, a software designed to provide generic services to shield the inherent dispersion and heterogeneity of the underlying infrastructure. The middleware enables data management, information services, executive management, and security services to function effectively. Typically, an information resource is utilized to keep comprehensive knowledge about all grid resources. Any aid has to be upgraded to be compatible with the present computing environment. The deployment of security resources is important to improve the security of resource accessibility inside institutions and to prevent the violation of local administrative and communication regulations. Data management resources are utilized to develop beneficial solutions that enable data accessibility, migration, replication, and integration. According to Sabahi,[14] executive management is applied to complete tasks by maximizing the utilization of accessible computing resources. Additionally, it is utilized to track the progress of a task and handle computation outcomes.

On the other hand, cloud computing is often utilized to provide resources via the cloud. Cloudware is a method of providing different factions depending on the type of cloud service provided. It is used to maintain current knowledge about available computing resources and create and manage virtual machines in response to users' requests. Cloudware can assist the implementation, setup, and deployment of applications and assure pricing, accounting, and user administration. Effective computing service usage involves techniques and rules identifying where to construct virtual machines and when to start and stop them depending on user preferences. Handa, A. et al. claim that user management is critical in ensuring real resource use.[6] Cloud computing protects users from complexity, allowing for easy usage and development. Cloud control is simple to operate because it is integrated with a single administration system.

Review of cloud computing

The technology is a highly effective resource accessible from a huge number of users and is extensively utilized around the world. It has a variety of dynamics, including abstract boundaries, scalability and ambiguity of location like the nature of a real cloud. The Cloud incorporates numerous information technologies, and technological developments have led the Cloud to grow and evolve. As defined by the National Institute of Standards and Technology (NIST), Cloud Computing is a technique that enables pervasive, easy and on-demand networking. It increases access to the common pool of computing resources configurations such as servers, applications, networks, and services, accelerating the provisioning process and reducing service providers' workload in engagement or management. Cloud computing includes five key characteristics, four deployment methods and three service methods.

Cloud computing integrates traditional computing tactics with networking methods, which consists of, but are not limited to, Utility Computing, Load Balance, Virtualization, Distributed Computing, High Availability, Network Storage Technologies, and Parallel Computing. The goal of Distributed Computing is to partition a broad task computation into manageable task parts; after that, a number of different computer users are assigned to analyze and gather all the results through the assembly. Parallel Computing tackles parallel issues that require great efficiency. It brings together considerable resources to compute and assess a certain task. Distributed Computing and Parallel Computing are compared in Figure 1.

Intrusion detection and prevention methodologies used by signature-based intrusion detection systems (SIDS)

Signature-based IDS operate by finding the specific patterns, such as a byte sequence in network traffic or instruction sequences known to be maliciously caused by malicious software (Malware). An alert is generated as soon as a signature that is constructed to perform intrusion aligns to a signature from a past intrusion – which now shows in a signature database. SIDS indicates that matching processes are used to find a coming intrusion. With SIDS, logs for the host are studied to find the variation of commands or performance that have been previously noted as malicious software.

SIDS has also been highlighted throughout recent and relevant academic research as Knowledge-Based Detection or Misuse Detection by Sedjelmaci H et al.[15] Additionally, Sarnovsky M et al. named signature-based intrusion systems as Knowledge-based Detection or Misuse concealment.[16]

Throughout Computer Science research, we can see that SIDS regularly performs an outstanding level of detection precision for future unknown intrusions. Although SIDS have been known to have complications in perceiving

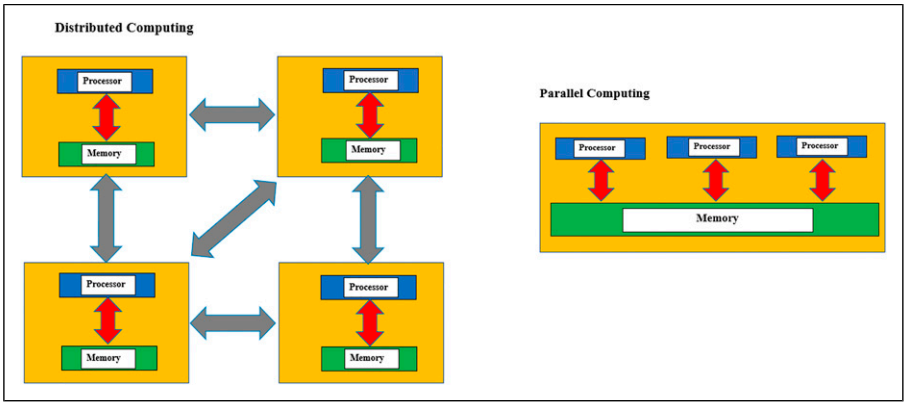

Figure 1. Comparison between Parallel Computing and Distributed Computing.

attacks known as 0-day, meaning there is no aligning signature in the database for anticipation of the signature of the new chapter being taken out and stored. SIDS are deployed in many common tools.

Traditional SIDS technology provides scrutiny to network packages and finds it difficult to compare in opposition to a database of autographs. However, the technology techniques are not advanced and capable enough to categorize cyber-attacks that cover a significant number of packets. There is a requirement for the IDS to recall the inside of past packets. Rumez M et al. noticed to generate a signature for SIDS, there are many techniques to construct a signature, including circumstances machines, formal verbal communication string patterns, language, and semantic surroundings.[17]

With an increasing rise of 0-day attacks, the SIDS technology has gradually become less successful over time due to there being no formal signature for this cyber-attack. Polymorphic deviations of the malware and the rising number of serious cyber-attacks can contribute to the destruction of the technological asset(s). A solution that could potentially be the successor of SIDS technology is AIDS technology, which delivers a good performance instead of focusing on what is different.

There are two variants of machine learning methods, and these consist of supervised and unsupervised machine learning techniques.

Intrusion detection – supervised learning technology

This section focuses on multiple supervised knowledge acquisition methods used in the field of IDS. Everything being shown in detail refers to literature presented throughout the paper.

Intrusion Detection Systems that adopt supervised learning methods could detect potential and definite intrusions using brand-named training data. With supervised learning Intrusion Detection Systems, every documentation works as a pair, carrying a network or host data and a connected output or value (label). This should be in exact intrusion or average modes. Supervised learning is known to consist of two phases known as "training" and "testing". In the first "stage" (training), applicable features and lessons are understood as the algorithm uses the data illustrations. When that is complete, feature selection has the potential to be functional for eradicating the redundant elements. The training data can be used for various methods. Supervised learning performance is utilized through an application to train the one carrying out classification activities, the classifier, to understand the crucial relationship between the input data and the labeled output value.

The significant differences of the supervised learning systems continue to be investigated through recent and relevant academic work, having their successes and constraints. In the "testing" phase, an eligible prototype categorizes the underived data into an "intrusion" or "normal" class. A consequential classifier shows a model that specifies particular values that forecast the class where the input data can be in the correct place. The presentation of the classifier in its capability to forecast the correct class is determined among the most significant systems of measurement.

Making categorization models that can perform simplification is an important task for the scholarship algorithm. There are various categorization methods which include: decision trees, rule-based systems, neural networks, support vector machines, Naïve Bayes, and nearest-neighbor. All procedures use knowledge-based methods that create a classification model. An ideal classification model will make use of the "training" data and correctly make out the class of records.

When focusing on decision trees, a decision tree is made up of three significant components. The starting element is a decision node, which is often used to classify a test attribute. The next element is a branch, where each branch stands for a likely decision based on the value of the test characteristic. The final element is a leaf that incorporates the class to

which the illustration fits. There are an array of various decision tree algorithms.

Intrusion detection – unsupervised learning technology

Unsupervised learning technology defines machine learning techniques that are used to obtain beneficial information from input datasets devoid of class labels. The input data places are often dealt with by unintended variables and a combined density model shaped for the data set. The output labels are prearranged with supervised learning and used to train the machine to get the required outcomes for an undetected data point.

As well as supervised learning, there are no labels specified, and as a substitute, the data is grouped in a robotic manner into a range of classes through the learning process. In the framework of developing an Intrusion Detection System, the unsupervised learning method uses machinery to understand intrusions by using unlabeled data to derive the model.

On certain occasions, the proceedings will be grouped together. Every possession that is in view in small groups is marked as an intrusion due to the average events that should fabricate a large number of groups compared to the anomalies. When analyzing the malicious intrusions and average occurrences differ, they do not go down into the unidentifiable group.

Purposes of intrusion detection and prevention systems

A common element of IDPS is that they cannot be utilized as a method to provide completely accurate recognition. When an IDPS incorrectly recognizes benevolent activity as malicious, a false affirmative has taken place. When an IDPS fails to make another grade to recognize malicious intent, a false unconstructive has, on the other hand, been established. It is not possible to eliminate false positives and negatives. For the majority of cases, mitigating the events of one augments the occurrences of the other.

Developing effective IDPS makes sure that the bay level derives from the intermediate level where automatic functions with real-time are established. In order to develop effective and efficient intrusion detection and prevention, there is a requirement that the bay level also is made up of an intermediate level where automated functions in real-time are performed.

Comparison between cloud data centre and traditional data centre

There are differences in the features of the traditional data center and the cloud data center. Radwan T et al. point although both types of data centers are in charge of presenting their tasks for execution, the traditional data center and the cloud data center has different configurations of hardware and software components for operation and services.[18] The traditional data center is defined by the security of its infrastructure in each task management. In addition, Pancholi VR and Patel B.P claim the physical infrastructure contributes to avoiding interactions between a variety of user aspects like networking, computation, and storage.[19]

The traditional data center has several features as follows: 1) It is supported by a variety of management tools; 2) it contains a number of patches and application upgrades; 3) it is comprised of an interweaved hardware environment that supports a variety of applications and platforms; 4) it is defined by the variety of hardware architectures and software that are supported; 5) it deals with highly complex tasks. The features of cloud data center consist of 1) there are few standard management tools; 2) it has very few updates and patches; 3) there are few dedicated applications; 4) it is composed of homogeneous hardware environments; 5) It deals with simple tasks; 6) it depends on a single cloud architecture.

As processes running in the private cloud use comparable system services, cloud infrastructure does not operate in an isolated paradigm. Each task makes use of comparable networking infrastructure, server system, and storage architecture. Cloud infrastructures benefit from software development that creates logical separation.

Cloud data centers are widely employed because they provide all the resources and functionalities offered by traditional data centers while being cost-effective due to economies of scale. Standard data centers are more flexible since it does not require the establishment of infrastructure ownership as a result of maintenance and administration. In traditional data centers, a gradual rise in storage capacity leads to an increase in complexity.[20] In comparison, cloud data centers are elastic and scalable, as any application can be served.

Features of cloud computing

Cloud computing methods are distinct from other forms of computing methods in their unique nature and features. According to Mahdavisharif M et al.,[21] the properties of cloud computing are divided into two categories: basic and essential features. This paper makes an explanation on the essential features:

1. **Accessibility of broad network:** Cloud services are made accessible using common procedures that enable users to access them via a variety of platforms and applications; for example, when sufficient IP network access is available, cloud services and resources are accessible at any time via laptops, mobile

phones, and personal computers regardless of the user's location.
2. **On-demand self-service:** This is a fundamental feature of cloud computing, which provides users with computing services in the form of network storage and server time. Depending on the request made by a user, cloud computing services can be provided at any time. On-demand self-service applies even in the absence of human interaction.
3. **Rapid elasticity:** Cloud computing provides elastic and fast computing capacity that facilitates instant scaling out and quick release too fast scaling in. The ability to deliver to customers only on request is not sufficient. The elasticity of cloud computing makes it possible to provide services in varying quantities at any given time. Elastically increasing service capacities during peak periods and reducing them during off-peak periods can decrease costs for cloud subscribers and effectively meet their expectations for quality of service.
4. **Pooling of resources:** Cloud resource providers bring together computing services to meet different users' computing needs with a variety of physical and virtual resources. This pooling of resources, such as storage servers and devices, is utilized by a large number of users. Cloud resource providers select the most suitable services from pooled resources for each cloud user's task to optimize service quality. Cloud resource sharing is the first option as it enables cost savings by allowing multiple apps to be developed in the cloud rather than using dedicated computing resources.
5. **Service measurement:** It is an automatic service that monitors and optimizes the use of a service and corresponds at a certain degree of abstraction to the type of cloud computing resources. Moreover, it monitors, controls, and reports on service utilization, leading to the actual purchase of resources.

Cloud computing delivery approaches

Cloud computing's delivery methods contain three layers (Figure 2), including Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). This paper makes a detailed explanation of the three layers in the following subsections.

The three levels of cloud computing are each explained below.

Platform as a service (PaaS)

Platform as a service facilitates cloud infrastructure deployment via customer-created apps developed by cloud computing providers' programming languages and tools. Users are not authorized to manage cloud infrastructures like servers, applications, data, networks, or storage; however, users can control applications placed in the application environment hosts. The application hosting environment ensures the rapid and transparent execution of programs. PaaS has a number of components, including web service delivery, database services, development platforms, and virtual desktops.[22]

PaaS has the following characteristics:

1. The same development environment is shared by numerous users.
2. Integrated databases and web services.
3. Different categories of application development services and application execution services are employed to facilitate the development, deployment, hosting, and testing of applications within an integrated environment.
4. These also include subscription and billing, managed by cloud computing tools.
5. Virtualization technology enables users to access the resources they need and dynamically scales them up or down as needed.

PaaS applies to the following types of individuals and organizations:

1. Enterprises looking to diversify their capital investment. PaaS enables cost savings related to computing infrastructure, application development, and execution. The companies that employ PaaS include Oracle Public Cloud, Microsoft Windows Azure, Google App Engine and Appends.
2. Developers who collaborate on the same product
3. Organizations that develop software using agile methods. PaaS reduces the difficulties related to fast application development and iteration.

Software as a service (SaaS)

Cloud Computing users are permitted to manage the cloud infrastructure under the SaaS delivery model, which is not the case with PaaS. The SaaS delivery model precludes cloud subscribers from authorizing cloud infrastructure and individual apps administration. Subscribers may lack sufficient access to configure apps. Enterprise resource planning, social networking, customer relationship management, data management, Email, and office productivity software are all included in the SaaS delivery model.[23]

The SaaS delivery method has the following characteristics:

1. Users of applications do not have to worry about hardware and software issues like patches and updates.

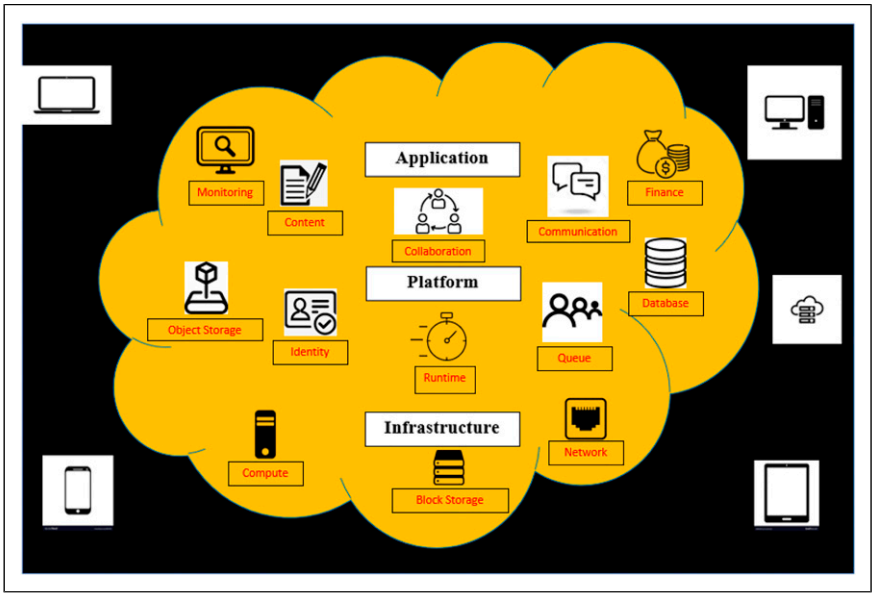

Figure 2. Delivery Approaches for Cloud Computing.

2. Application management is based on a central site.
3. APIs are employed to achieve integrated applications of third parties.
4. The software server is hosted remotely and accessed via a web browser over the internet.

SaaS applies to the following types of services and organizations:

1. Applications that require internet and mobile access, including sales management software and CRM system
2. Collaboration for short-term projects. Due to the definition of the pay-as-you-go model, it is inconvenient to set up and close a collaborative environment swiftl
3. Applications that have a clear rise and fall in demand. For example, hotel bookings have great demand during holidays and demand for tax software is high during peak periods of tax filing.
4. Companies that are just starting need to put their e-commerce websites in operation quickly.

The examples of Software as a Service included Cisco Web Ex: Oracle Public Cloud, Concur, Google Apps, Microsoft Office 365, Workday, Salesforce.com, and Citrix GoTo Meeting.

Infrastructure as a service (IaaS)

Cloud computing capabilities are employed to provide users with computing resources and services, consisting of networks, content delivery, storage, backup and recovery, and processing. They also assist users with the implementation and operation of their own software. In IaaS, users are not authorized to manage the cloud infrastructure, and they are only allowed to manage operating systems and deploy applications. In IaaS, users have limited rights to manage host firewalls.[24]

The features of IaaS are as follows:

1. It uses a single piece to connect several different users on hardware.
2. It has dynamic scaling abilities, the cost of which varies based on the choice of infrastructure.
3. It is made up of resources that are frequently available for use.

IaaS applies to the following types of organizations:

1. Organizations that are in growth but do not know which applications are right for them. The development of these organizations is unpredictable, and they are not yet ready to commit to a specific infrastructure.
2. Upcoming and small firms that do not need to spend a lot of money and time on hardware and software.
3. Organizations that demand full software management.
4. Organizations with unstable demand are even more critical for various dynamic scalability depending on the traffic troughs and spikes.

The companies that employ the IaaS model consist of Microsoft Azure, Amazon Web Services (AWS), IBM

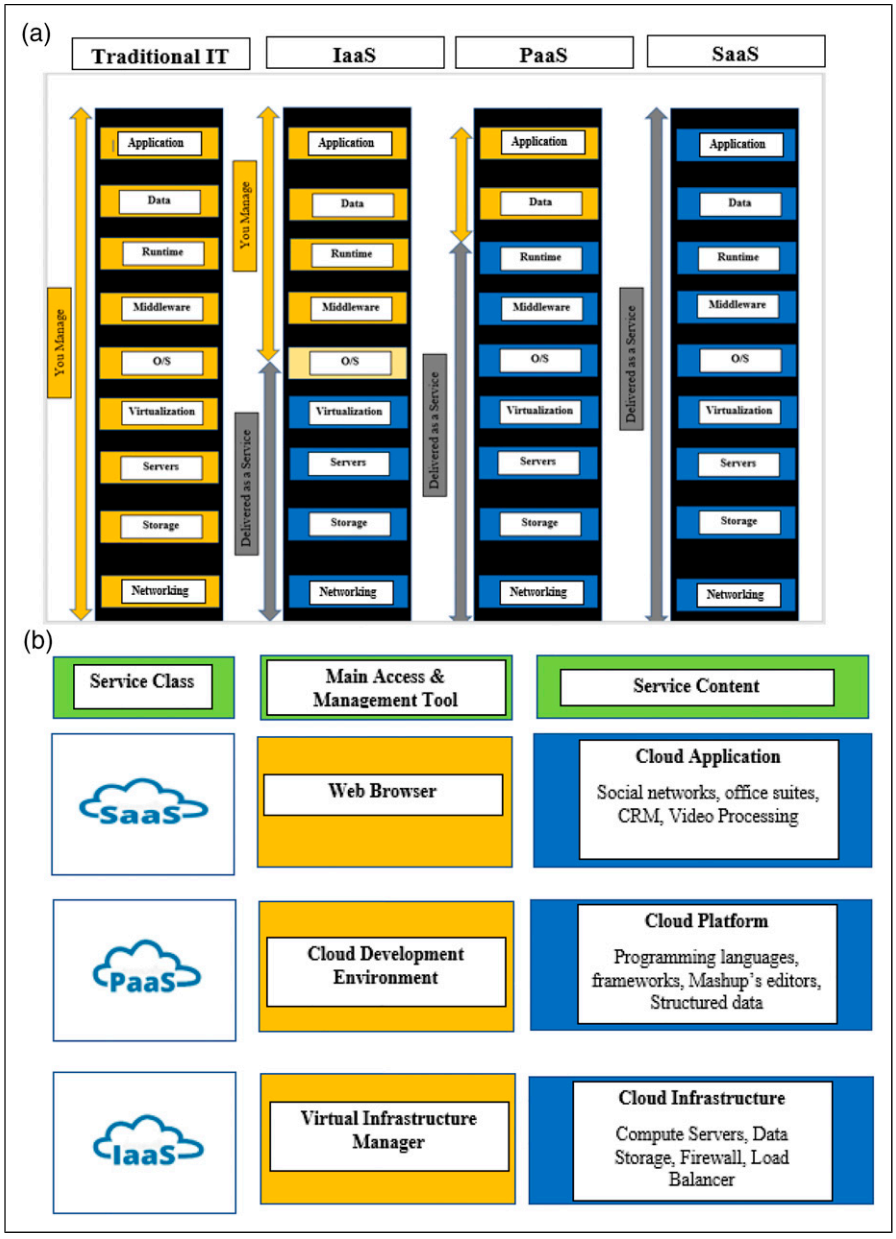

Figure 3. (a,b): The Responsibility Separation of Software-as-a-Service, Infrastructure-as-a-Service, and Platform-as-a-Service.

Smart Cloud, Cisco Metapod, Verizon, GoGrid, and Google Compute Engine (GCE).

Figures 3(a) and (b) below show how the three levels of responsibility are separated in SaaS, IaaS, and PaaS in comparison to traditional information technology.

Cloud computing deployment approaches

Cloud computing has four deployment methods: public, private, hybrid, and community.[25] The models differ from one another because they have various features and implications for users. The deployment strategy is determined by the business goals and requirements. A company must conduct performance, security, and reliability reviews to select the best deployment strategy.

Public clouds

Public clouds are often regarded as the ideal deployment strategy, and a number of users name them as clouds. Public cloud services are made available to the public and managed by cloud computing resource providers. Cloud

infrastructures can be deployed through data centers and high-speed networks. A public cloud is distinguished by its multitenant capabilities; users are different, and their data is not publicly accessible.[26]

Public clouds include several advantages as follows:

1. **Readily affordable**: Because public clouds only require users to pay for the things that can be viewed, it is low-cost. The cost of expanding or downsizing an organization is proportional to its size. In comparison, a cloud infrastructure may be required for a private cloud designed to cope with more expensive expansion; cost savings will not occur in the event of scaled-down demand. Other considerable cost savings are associated with the size and work of the in-house IT grou
2. **Efficiency improvement:** Because public clouds have teams that are dedicated to the maintenance of the infrastructure, the difficulties related to downtime are not likely to arise. As long as the cloud provider hosts an application, the provider normally manages the updates, which saves on upgrading costs.

Public clouds contain several shortcomings as follows:

1. **Insecurity factor:** Many organizations that have adopted high-level versions of public clouds have demonstrated potential security issues in public clouds. There are ineffective security issues when cloud computing providers own public clouds, aware of security challenges and their impacts on user perception.
2. **Outdated cloud computing Provider:** If cloud computing providers do not upgrade the hardware regularly, cloud customers are vulnerable to the issues of compliance and execution speed.
3. **Decreased control:** Since cloud computing providers manage entirely public clouds, consumers do not have the

Permission to get administrator rights and perform tasks with full controls. On the other hand, users are authorized to manage over the cloud with full permissions in the private cloud.

Private clouds

Private clouds can be obtained by either leasing or ownership, without security standards, bandwidth restrictions, or legal obligations. The computing infrastructure in a private cloud is specifically provided for an organization and is not allowed to be shared with other organizations.[15] When enterprises are not able to host their data remotely, both cloud computing providers and users have the optimal infrastructure and security management. They elected to utilize private clouds to improve resource automation and usage. [16]

The following are some of the benefits of using a private cloud:

1. **Flexibility and control:** Private cloud enables organizations to have total control over clouds to deploy new applications; it allows for rapid transformation.
2. **Effective performance:** Private clouds are deployed within the firewalls of organizations, resulting in greater performance than public cloud resources.
3. **Security aspect:** Private clouds are thought to provide a greater level of security than public clouds since security is managed within the organization. However, this is not to say that private clouds are free from security problems. The primary distinction between public and private clouds is that public clouds are often more appealing in terms of penetration than private clouds because of their enormous volume of data.

Private clouds contain several shortcomings as follows:

1. **Need for Additional Maintenance:** When software providers do not maintain private clouds, enterprises can benefit from daily upgrades in conjunction with current software as service applications.
2. **Increased costs**: In comparison to public clouds, a private cloud is a costly method in every way, implying that the organizations spend more on procuring private cloud-related services than public cloud services. The management expenses of private clouds are also substantial.

Community cloud

The concepts of community clouds and public clouds can be easily confused. Community clouds provide resources to individuals and groups with the same interests, whereas users of public clouds do not have similar interests. The computing infrastructure is on-site or off-site in a community cloud. In contrast to public clouds, where ownership and management are under the individual supplier or owner, community cloud resources are owned and managed by one or more community contributors.

Hybrid cloud

The hybrid cloud strategy is a combination of the above-mentioned deployment methods.[16] In a hybrid cloud, a management framework aids in assuring a single cloud environment. Organizations are drawn to hybrid cloud

methods due to the rising need for pricing, performance, and security.

Barriers preventing adoption of cloud computing

The deterrents that may prevent or delay organizations from employing a cloud computing strategy are listed below.

1. **Security/Privacy issues:** The majority of organizations are concerned about the security and privacy implications. However, some do not feel that security concerns are an insurmountable barrier or that there are no viable solutions.
2. **Resistance within the organization:** Cloud computing is an essential strategy as it minimizes the administrative tasks performed by back-end IT systems, leading to increased workloads for front-end workers. In addition, this may result in a large reduction in the amount of the IT department's workforce, which could be further perceived as a threat by the department's expertise. The organization's employees, in turn, become fearful of losing their jobs and management of critical systems.
3. **Service Level Agreement, Quality of Service, and Governance:** There is a lack of proper control of IT and service lifecycles in the cloud.
4. **Trustworthiness and Reliability:** Outages in the cloud system have taken place at Amazon and Google; documentation and publicized cloud outages prevent large enterprises from employing cloud computing methods.
5. **Interoperability and integration:** At present, standards for APIs and cloud computing interfaces, related technical standards, as well as standards to realize interoperability from private to public or public to private clouds are not well developed.

Barriers to Cloud Computing deployment can be observed in the work of Jangjou M et al., 2022 where there is a strong focus on the Cybersecurity risks when adopting Cloud Computing technology in both client and server-side layers of Cloud architecture.[26] These risks include Providing vulnerable APIs to Cloud users, lack of awareness of the occurrences of security incidents, limitations of the cloud user to one CSP, lack of service provisioning by the CSP, Account theft, Phishing attacks, Malicious employees, Information gathering, and dependency to the CSP. The Cybersecurity risks to the Cloud systems are ranked, where the risks are ranked from 'Low', 'Medium' and 'High' measured against the 'Probability', 'Impact', and 'Frequency'. When analyzing these risks, we can notice that the particular risks of 'Limitation to one CSP' and 'Account theft' show to be the most concerning cybersecurity issues of utilizing the technology in a business. This research can be optimized when deploying this innovative infrastructure and systems into the strategy of a business.

Achievement and factors affecting the cost

The adoption of cloud computing is constrained by several factors as follows:

1. **Service Level Agreement:** Before utilizing computing cloud services, a user must sign a service level agreement, which details the information about the user's request and the computing provider's abilities, fees, etc.
2. **Security:** Effective security improves the efficiency and effectiveness of all cloud systems, serving as a supporting component to system protection.
3. **Networking Bandwidth:** The performance of cloud computing is often reduced because of insufficient bandwidth, which results in the inability to offer essential resources at any given moment.
4. **Many consumers:** When the number of users is greater than the capacity of the cloud, the performance of the cloud service is usually in a poor state.
5. **Fault Tolerance:** Cloud computing should provide resources and backup for services. Fault tolerance allows performance improvements in cloud computing.
6. **Data Recovery:** Cloud computing can retrieve any data that has been lost, damaged, or corrupted, allowing for effective functioning.

Other aspects like processing power, scalability, redundancy, workloads, and latency affect cloud computing performance adversely or favorably.

A practical assessment of the total cost of ownership (TCO) of cloud computing resources is recommended. TCO contains all expenditures associated with cloud computing resources during their lifespan, from acquisition to disposal. There are two types of ownership costs associated with cloud computing services: direct and indirect expenses. According to Basu, direct expenses include licensing fees for hardware and software, utility costs regarding bandwidth and resources, as well as resource management costs.[27] Indirect expenses are a subset of ownership costs, including employment costs for coordinating cloud computing and associated applications and negotiating and managing a cloud computing service.

The barriers around the cost to the implementation of Cloud Computing as a strategy for a strong system solution into the organization can be observed in the recent work of Abdlrazaq, A. and Varol, A., 2021, where the researchers conducted investigations on Cloud Computing.[28] They defined some of the main benefits around how enterprises

and customers receive a decrease in hardware costs once they begin using Cloud-based services due to not requiring any powerful computers that meet specific capabilities - due to the removal of reliance on storage and power processing. As well as the removal of enterprises relying on paying for upgrading their software to the latest version due to the Cloud provider taking responsibility for upgrading the applications automatically in the Cloud environment can also be seen with the decreased maintenance cost - including software and hardware upgrades. One of the most attractive cost-saving methods when adopting Cloud technology is the ability to avoid income tax by operating expenses over capital expenditures by renting the devices from the vendor rather than buying them directly.

Organizational adoption

Teesside university

Teesside University is a Higher Education institution that delivers an array of technology courses and degrees ranging from Level 4 to Level 8 and is active in research and scholarly activity. Cloud computing is an essential part of the curriculum delivered and is usually embedded into many computing modules. Teesside University has also produced many scholarly articles around cloud computing and cybersecurity. The students learn through scheduled formal lectures and lab sessions, which contain a blend of theoretical and practical tasks to engage the students in the subject area. The students study cloud-based architecture throughout many modules to understand the design, development and configuration of Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS).

University of sydney

In the research of Chandran D and Kempegowda S, we can observe a hybrid E-learning platform being proposed for teaching based on a cloud architecture model.[29] The main motivation for this proposal was the ability to reduce costs and provide a dependable data storage and data sharing environment. Through this research, it has been noticed that the cloud can provide significant possibilities for the users in contrast to just using local infrastructure. The cloud delivery model consists of three layers, including (1)The Infrastructure Layer - consisting of hardware, network infrastructure and monitoring tools, (2)Platform Integration Layer - consisting of virtualization instances and (3)Application Layer - consisting of various applications such as social networking. The proposed solution aims to evolve and innovate all three layers to provide a better service - revamping the infrastructure with new systems to meet the changes in technology. For example, old software might be unable to run on older hardware. They aim to provide a migration to cloud systems to a virtual environment. Still, for speed, they understand that not all applications can be moved from local hosting to cloud-based hosting. Hence, they aim to keep teaching and learning activities with high computational power on the University side.

Middlesbrough college

Middlesbrough College is a Further and Higher Education institution that delivers an array of technology courses ranging from Level 1 to Level 6, including Foundation and Undergraduate Degree Programs. Cloud computing is a significant element of the curriculum taught at all levels. The institution teaches cloud computing in a conceptual method where students design, develop and produce diagrams of the infrastructure used to provide one of the following functions: Software-as-a-Service (SaaS), Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS). The students learn through active blended learning making use of lecture slides, formal lab-based activities and informal lab-based activities. The students are assessed by a mixture of assignments and examinations at all levels.

National health service

The National Health Service (NHS) is adapting to the growing demand for organizational Cybersecurity measures. They have implemented system-wide monitoring capabilities through cloud-based technology centrally as a business to improve the cybersecurity measures in their digital strategy.[30] They have introduced Windows Advanced Threat Protection (ATP), which allows them to monitor the threats and vulnerabilities on all individual machines across thousands of branches. More than one million devices are currently being used in the NHS, with around 73% being defended by this strategy. The first trust to implement this technology was Morecambe Bay in May 2018. Using this detection and prevention technology will allow the NHS to see when a user has opened a potential phishing email containing malicious software (Malware). They can then work backward to understand what the user was doing previously. The alerts produced by this technology will provide information about the damages the malware has caused and which machines it has attempted to harm.

Banking

In the recent work of Banking, there has been an investigation of Intrusion detection used for internet banking and a novel architecture proposed.[31] The key cyber attacks the authors focus on as an issue to solve with intrusion detection

and prevention technology include Phishing attacks, Pharming, Man-In-The-Middle (MITM) attacks and Man-In-The-Browser (MITB) attacks. The architecture they propose to defend banks against cyber attacks is derived of firstly understanding the networking security measures that banks are deploying - making sure they are utilizing Firewalls to block everything except specific traffic allowed paired with an Intrusion Detection System to mitigate the vulnerabilities in Firewall technology and provide an extra layer of defense. The second part of the cyber defense architecture for banks uses the IDS in three different places - these include deploying a Host-based IDS on the users' personal computers (HIDS: Client-side). The HIDS for internet banking uses a database of the bank's client attack patterns. In addition, using a Network Intrusion Detection System (NIDS), which sits between the Firewall and the Internet Banking Systems (on the internet banking systems side) - when using the NIDS for internet banking this uses a database of the banks attack patterns and monitors the banks network traffic by using both anomalies and a misuse based detection method. The final IDS is a Special host Intrusion Detection System (ShIDS) on the banks' server, which provides internet banking services and processes individual transactions. It is for the banks' internal servers, which have databases associated with the banks' financial servers' attack patterns - this works by monitoring the bank server traffic and using a hybrid technology based on anomaly detection and misuse detection with a reactive response system. The proposed security solution for banks increases the security and consistency of internet banking services and reduces the damage of fraud events.

Google

Google's cloud architecture is currently being used to migrate mobile and web applications observed in Kumar.[32] Google's Firebase cloud database service does appear very popular with app developers currently. The integration of Android Studio makes it an attractive Platform-as-a-Service (PaaS) for developers. The cloud environment has a shared responsibility model where users can secure their own database with an appropriate access control policy. However, there are growing concerns when using the Firebase cloud architecture due to the more widespread database access control misconfigurations that are becoming more popular and attracting malicious users. Due to the platform's vulnerabilities discussed, the authors have developed their own open-source static analysis plugin tool to check the accessibility of the Firebase databases used in an app in the development process.

Facebook

We can notice a showcase of a cloud computing architecture for social computing in recent literature. The researchers demonstrate five architecturally needed components to perform social computing; these include service providers and consumers, services offered, local services, physical elements, and cloud computing platforms. They also discuss the four different social networks available: Social networks, Services networks, Cloud computing networks, and physical thing networks. Facebook works in the social cloud by mapping services to particular users through Facebook identification which allows for the definition of unique policies with the interaction between users.

IBM

To defend their cyber infrastructure from incoming attacks, IBM can utilize LSTM deep learning algorithm as demonstrated in recent academic literature from Mahdavisharif, M et al.[21] The authors explore using the LSTM algorithm as a means for Intrusion Detection for the business. They have investigated that if there was a combination between the algorithm and the NSL-KDD dataset, we would be able to train normal behavior to recognize known attacks or new attacks from normal behavior. The results gathered from the simulation demonstrate that the use of big data techniques and algorithms can increase the accuracy and rate of detection whilst also reducing the rate of false alarms - which is a determining factor in anomaly-based intrusion detection devices.

Alibaba

Alibaba is the largest Infrastructure-as-a-Service (IaaS) provider in China. They provide cloud computing services primarily to external small and medium-sized enterprises (SME) customers and internal departments of the Alibaba Group. Alibaba has developed a cloud architecture for deploying its cloud platform to improve the performance of its cloud servers and to be able to support both internal and external use.[33] AliYun, as a latecomer, extensively replicated the technology used by Amazon, including knowledge of key technical components such as system architecture, APIs, and algorithms.[34] AliCloud launches Elastic Compute Service (ECS). This scalable IaaS service provides consumers with a more flexible way to use high-performance cloud servers, customize hardware specifications of servers according to needs, and scale computing resources on demand. When utilising the LTSM algorithm they observed the ability to recall information with long-term and short-term time dependancies highlighting the ability of detecting planned attacks to the network.

Tencent

In the early days, Tencent Cloud was not a separate project and was used more for Tencent's internal gaming

development. It has been in high growth after Tencent Cloud as a separate project in 2012. Tencent Cloud has always been slower than AliYun in terms of development due to the lack of business experience. Tencent has a wide range of cloud computing services, including Cloud Virtual Machine, GPU Cloud Computing, CVM Dedicated Host, Auto Scaling, and Batch Compute. GPU Cloud Computing is much more powerful than traditional CPU cloud computing. They provide powerful single- and double-precision floating-point computing power, with the peak computing power of 125.6 T Flops for single-precision floating-point and 62.4 T Flops for double-precision floating-point.[35] Using numerous efficient arithmetic logic units (ALU) to support parallel processing and massively parallel throughput can be achieved with multiple threads.

Framework for organizational adoption

Cloud computing can be a significant innovation for businesses, but it is essential to understand what methods of cloud computing adoption are appropriate and the best opportunity for the business to make. The types of cloud computing include:

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

Following our framework should help users decide which cloud-based technology suits their organization.

- Understand what the current technology and services are deployed

The organization should first understand what current technology is being deployed in their business ranging from network infrastructure to applications, files and storage. When analyzing their current state, they can begin to understand their opportunities for moving forward with the technology.

- Understand what cloud technology is appropriate for the business

The organization should then understand what current technology deployed are they want to move to the cloud to understand what innovations they are hoping to achieve. For example, applications that require a significant amount of computational power might be kept locally. In contrast, files might be moved on to cloud architecture, but suitable applications to be kept on the cloud environment, such as collaborative web application software used for projects.

- Understand what cloud features you expect to use

Users and adopters should next understand the cloud features you are hoping to achieve with your innovative deployment strategy. For example, accessibility of a broad network, on-demand self-service, rapid elasticity, service management and pooling of resources are crucial. Users and adopters should understand the motivations and strategy they hope to achieve by investing in cloud architecture for your business.

- Understand what cybersecurity measures can complement your cloud

Businesses also need to understand that when changing and upgrading their infrastructure, cybersecurity measures need to be contemplated - one of the most common cybersecurity measures is an Intrusion Detection and Prevention system to monitor and block malicious traffic. Deploying cloud architecture can pose further security risks due to keeping the infrastructure off-site but can also mitigate other security risks by giving the provider the responsibility for the security.

- Understand the costs and your budget

Users and adopters have to understand the costs of your budget to determine how much cloud computing innovation you will be pursuing for your business - for example, a hybrid approach may be a significantly lower cost due to being able to use older technology and systems that the company might already be in possession of or if it is a startup company a full cloud architecture might be the cheaper option as a subscription service instead of buying infrastructure and having the cost of maintenance, storage and security.

Future research directions

We propose for future research directions using the new Seed labs internet emulator to design a testing environment where will be producing a software-defined network written in python code that contains cloud-based infrastructure to understand how the cloud can be deployed in the new environment and perform analysis, experiments and results to provide a contribution through published journey article to the scientific community. With the technology deployed and working, we can then look at the cybersecurity landscape and perform penetration testing with countermeasures and a defense strategy. We also aim to explore the many organizations adopting different cloud computing

technology to enhance their business by providing new security measures or services.

Conclusion

Throughout this paper, we have focused on the organizational adoption for cloud computing - this can include services and different security measures that businesses can invest in to innovate their companies' technological capabilities. We look at three different key sectors, including Further Education, Higher Education and Healthcare, for the businesses that have adopted the technology and how they are using it individually. We convey the many different types of network topologies available while also reviewing the different types of cloud architecture that can be deployed, such as a public cloud, private cloud, community cloud and hybrid cloud. We also explain various cloud features and services are that are offered, including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS).

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work is supported by VC Research (VCR 0000170).

ORCID iD

Victor Chang https://orcid.org/0000-0002-8012-5852

References

1. Tavbulatova ZK, Zhigalov K, Kuznetsova SY, et al. July. Types of cloud deployment. *J Phys Conf Ser* 2020; 1582: 012085.
2. Wang LC, Chen CC, Liu JL, et al. Framework and deployment of a cloud-based advanced planning and scheduling system. *Robotics and Computer-Integrated Manufacturing* 2021; 70: 102088.
3. Liu Z, Sampaio P, Pishchulov G, et al. The architectural design and implementation of a digital platform for Industry 4.0 SME collaboration. *Comput Industry* 2022; 138: 103623.
4. Aldwairi M, Khamayseh Y and Al-Masri M. Application of artificial bee colony for intrusion detection systems. *Secur Commun Networks* 2015; 8: 2730–2740.
5. Butun S, Morgera D and Sankar R. A survey of intrusion detection systems in wireless sensor networks. *IEEE Commun Surv Tutorials* 2014; 16: 266–282.
6. Handa A, Sharma A and Shukla S.K. Machine learning in cybersecurity: a review. *Wiley Interdiscip Rev Data Min Knowl Discov* 2019; 9: e1306.
7. Gupta H and Sharma S. Security Challenges in Adopting Internet of Things for Smart Network. In: 2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 18–19 June 2021, pp. 761–765.
8. Khraisat A, Gondal P, Vamplew P, et al. Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics* 2020; 9: 173.
9. Huang M, Liu A, Xiong NN, et al. An effective service-oriented networking management architecture for 5G-enabled internet of things. *Comput Networks* 2020; 173: 107208.
10. Cirnu CE, Rotună CI, Vevera AV, et al. Measures to mitigate cybersecurity risks and vulnerabilities in service-oriented architecture. *Stud Inform Control* 2018; 27: 359–368.
11. Zissis D and Lekkas D. Addressing cloud computing security issues. *Future Gener Comput* 2012; 28: 583–592.
12. Tripathi BS, Gupta R and Reddy SR. Cloud architecture based learning kit platform for education and research–a survey and implementation. In: International Symposium on Ubiquitous Networking 2021, Limoges, France, 20–22 November 2019, pp. 172–185.
13. Yangui S, Goscinski A, Drira K, et al. Future generation of service-oriented computing systems. *Future Generation Computer Syst* 2021; 118: 252–256.
14. Sabahi F. Cloud Computing Security threats and responses. IEEE 3rd International Conference on Communication Software and Networks, Xi'an, China, 27–29 May 2011, pp. 245–249.
15. Sedjelmaci H, Senouci SM and Abu-Rgheff MA. An efficient and lightweight intrusion detection mechanism for service-oriented vehicular networks. *IEEE Internet Things J* 2014; 1: 570–577.
16. Sarnovsky M and Paralic J. Hierarchical intrusion detection using machine learning and knowledge model. *Symmetry* 2020; 12: 203.
17. Rumez M, Grimm D, Kriesten R, et al. An overview of automotive service-oriented architectures and implications for security countermeasures. *IEEE Access* 2020; 8: 221852–221870.
18. Radwan T, Azer MA and Abdelbaki N. Cloud computing security: challenges and future trends. *Int J Computer Appl Technology* 2017; 55: 158–172.
19. Pancholi VR and Patel BP. Enhancement of cloud computing security with secure data storage using AES. *Int J Innovative Res Sci Technology* 2016; 2: 18–21.
20. Naik N and Jenkins P. An analysis of open standard identity protocols in cloud computing security paradigm. In: IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress

(DASC/PiCom/DataCom /CyberSciTech), Auckland, New Zealand, 8–12 Aug. 2016, pp. 428–431.
21. Mahdavisharif M, Jamali S and Fotohi R. Big data-aware intrusion detection system in communication networks: a deep learning approach. *J Grid Comput* 2021; 19(4): 1–28.
22. Khalil I, Khreishah A and Azeem M. Cloud computing security: a survey. *Computers* 2014; 3: 1–35.
23. Ye N, Emran SM, Chen Q, et al. Multivariate statistical analysis of audit trails for host-based intrusion detection. *IEEE Trans Comput* 2002; 51: 810–820.
24. Hussein NH and Khalid A. A survey of cloud computing security challenges and solutions. *Int J Computer Sci Inf Security* 2016; 14: 52.
25. Chen D and Zhao H. Data security and privacy protection issues in cloud computing. In: International Conference on Computer Science and Electronics Engineering, Hangzhou, China, 23–25 March 2012. IEEE, 2012, 231, pp. 647–651.
26. Jangjou M and Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. *Arch Comput Methods Eng* 2022: 1–22.
27. Basu S, Bardhan A, Gupta K, et al. Cloud computing security challenges & solutions-A survey. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, 8–10 January 2018. IEEE, pp. 347–356.
28. Abdlrazaq A and Varol A. Cloud computing's impact on enterprises in term of security and cost. *Int J Security* 2021; 12(1): 1.
29. Chandran D and Kempegowda S. Hybrid E-learning platform based on cloud architecture model: A proposal. In: 2010International Conference on Signal and Image Process, Chennai, India, 15–17 December 2010. IEEE, pp. 534–537.
30. NHS Digital. How we're improving Cyber Security - NHS Digital. https://digital.nhs.uk/blog/transformation-blog/2019/update-on-nhs-digital-cyber-security (2022, accessed 29th January 2022).
31. Banking A. A proposed architecture of intrusion detection systems for internet banking. https://silo.tips/download/a-proposed-architecture-of-intrusion-detection-systems-for-internet-banking (2022, accessed 29th January 2022).
32. Kumar A. *Mastering firebase for android development: build real-time, scalable, and cloud-enabled android apps with firebase*. Birmingham, UK: Packt Publishing Ltd, 2018.
33. Zhang G and Ravishankar MN. Exploring vendor capabilities in the cloud environment: A case study of Alibaba Cloud Computing. *Inf Management* 2019; 56: 343–355.
34. Ahmad ES. *Infrastructure as a service: a practical study of alibaba cloud elastic compute service (ECS)*. Syrian: Report, Tartous University, 2019.
35. Cloud Tencent. GPU cloud server, https://cloud.tencent.com/document/product/560 (2022, accessed 2nd Feburary 2022).