Al-Rafidain Journal of Engineering Sciences Journal

homepage https://rjes.iq/index.php/rjes

ISSN 3005-3153 (Online)

Cloud Computing and Its Security in Real applications

Mohammed khodayer Hassan[1,*] Aymen Mohammed Khodayer[2] , Omer Mohammed Khodayer[3], and Maiduc-Alexandra[4]

[1]Department of Computer Technical Engineering, Al Rafidain University College, Baghdad, Iraq
[2,3] Department of communication Technical Engineering، AL – Farahidi University, Baghdad, Iraq
[4] Department Director for management of Scientific Research, University Polytechnical of Bucharest, Bucharest

ARTICLE INFO

Article history:

Received	09 April 2024
Revised	15 April 2024
Accepted	02 June 2024
Available online	04 June 2024

Keywords:
Cloud computing,
Cloud Resources,
Cloud data storage,
Cloud data security,
Cloud challenges.

ABSTRACT

This study article aims to investigate the characteristics of cloud security risks and ways for reducing their impact. Furthermore, there are difficulties associated with the effects of these concerns on information technology. The goal was to identify many substantial dangers and assess solutions to mitigate them. The text outlines some prevalent risks associated with cloud computing security, including distributed denial-of-service (DDoS) assaults, account hijacking, malware attacks, and data breaches. Although there are obstacles, there are significant advantages associated with the cost savings, scalability, and superior performance of cloud computing via the internet. Various solutions have been adopted, including the adoption of shared responsibility and the use of developing technology. Cloud computing is a system that enables users to remotely access computing resources via the internet, rather than relying only on locally accessible on-site computers. The cloud providers have the responsibility of assuring the confidentiality and security of the cloud computing infrastructure, while the customers are responsible for safeguarding their applications and data. Cloud computing is particularly advantageous for organisations since it effectively addresses the challenges of local data storage and restricted data access. These resources, such as memory management, number of processors, and nodes, may be easily delivered and released with little management efforts or via interactions with a service provider. The emerging security system is used to address novel cyber threats.

1. Introduction

The phrase "cloud computing" refers to a network of interconnected servers and has gained significant popularity in recent years. Utilizing a public cloud provider's cloud computing service involves hosting data and applications with a third party, which distinguishes it from conventional IT where data was mostly stored inside a self-managed network. Transporting computer resources over Cloud computing refers to the utilization of various internet resources, including processing power, storage, databases, analytics, software applications, and artificial intelligence. Cloud computing may be used without limitations anytime there is a need for it. Cloud computing is a framework that offers computing resources, such as servers, storage, databases, and software applications, via the internet instead of relying on local hardware and infrastructure. Consequently, users have the ability to retrieve these resources from anywhere, at any time on any device with an internet connection.

Cloud computing is a way to access information and applications online instead of

[*] Corresponding author E-mail address: drmohammednofa@gmail.com

https://doi.org/10.61268/gmqmnm28

having to build, manage, and maintain them on your own hard drive or servers. It’s fast, efficient, and secure. It works on demand delivery with pay-as-you-go internet pricing, and the charge will vary according to the resources and data used which is automatically measured. This technique can replace buying, owing, installing and maintaining physical material on-premises. Cloud computing has changed the way of life; it shows a great advantage for both customers and organizations, and playing significant role in the future of information technology (agile, efficient, and rapid technological change). Cloud computing has platform to provide AI and machine learning applications. This enables organization to build and deploy their own technologies easily with low cost. Beside that cloud computing has heavily investment in security branch to avoid cyber threats. The architectural configuration of cloud computing can handle many types of workloads while previous application was optimized for specific cluster.

Cloud computing can help organizations to scale their information technology resources easily according to the demand or changing business needs and market conditioning without heavy duty for changing in hardware equipment’s or software programming, that would help to reduce the infrastructure costs and improve operational efficiency. Due to constantly evolving in cloud computing landscape, many organizations have faced complex challenges to stay competitive with others. The agility and adaptability in cloud technology leads to new, way of working (operating, accessing, storing and manipulation) and you can access the data from anywhere over the internet. The payment only for the usage of the resources rather than investing on expensive hardware and software on site. The Cloud computing has many advantages in helping firms and organizations by solving their problems through, collating, storing and analysing the data which has stored in large data base.

A further step forward is an accomplished by storing data in graphics processing units **(GPUs),** which helps to process data in parallel form on cluster of machines. Many types of operations can be programmed to run on GPUs. This trend is taking good place in the development environment during these coming years. These changes will develop how to store, compute and use data in the near future change to enhance the type of business system. Cloud computing has a wide spread use by many organizations because of its flexibility and scalability. It is used for many routine tasks (data analytics, virtual desktops, data protection and software development). The big competition among AWS, Microsoft Azure and Google cloud platform have taken a crucial issue to implement and apply the cloud computing in the market during this year 2024. So, organizations need to run many numbers of algorithms parallel on cluster of machines, to achieve real-time analyses. By this method, the Cloud computing can help organizations to get more computing resources in a flexible, and easy way [1].

2. Emerging Trends in cloud security and its Development

Many new trends are emerging in cloud security. One of these is containerization technology that includes software and applications in portable containers that provide isolation and independencies from another surrounding environment [11]. By implementing this technology, the sensitive data of organization has to be insured within the container. Another type of emerging trends in cloud’s security is server less computing, which helps to create and run application without using servers or any backend infrastructure [12].

In this type, it is essential to establish seamless communication between server less function with the other application architecture to maintain good performance and ensure high level of security. Artificial intelligence and machine learning (ML) are utilized to ensure cloud security. These techniques are automated and have a great effect to enhance the performance of cloud servers, and mitigate the effect of threats. Quantum computing (QC); in this type user can access online different quantum resources to perform quantum algorithms without using specialized hardware [14]. Quantum computing is used to solve complex computational problems and its integration into cloud infrastructure leads to implement the cryptography to limit or overcome the vulnerabilities in the system. So the encryption algorithms are very important to protect sensitive data in the cloud computing.

The development of computing system started from the Main frames computers that are used by different organization, to solve many complicated problems such as financial transaction processing, census, industry applications and consumer statics. Distributing computing system in this type the components of the software are shared among multiple different computers and computer on different networks can communicate with each other by sending messages between them to perform a certain task by providing faster computational speed. Cluster computing refers to many computers connected together to a network to perform a certain single entity complicated task by providing faster computational speed and enhanced integrity of each node in the system. Grid computing this type of form is consisted of many clusters network which are connected in loosely coupled and they are working in distributed form and parallel computing [2].

3. Impact of Emerging Technologies on Cloud Security

Due to the fast development of the emerging technology, which has a highly effect on the cloud computing security. The using of server less and containerization are enhanced the performance of cloud server through the agility and scalability of the cloud server [15]. Various migration strategies are used to overcome the diverse security challenges which considered as a part of the vulnerabilities. Regular scan of vulnerabilities can help assess company’s security level. The use of ML and AI need mitigation strategies also. The ML needs to be up dated always otherwise security attach may occur. Cryptographic algorithms are used in cloud computing to reduce the risk of attacks. However, conducting regular assessment for all companies to ensure the cloud security.

4. Quantitative Analysis of Threats and Mitigation Strategies

Mathematical models and statistical methods can help and facilitate the quantitative analysis of the cloud security mitigation strategies. Probabilistic risk assessment (PRA) is one of suitable method to implement for this case [17]. PRA is used to evaluate the effectiveness of the methods which are implemented in identifying and mitigating cloud security. The likelihood of security problem issue can be calculated by the quantitative technique PRA. For example, assume that PRA indicates 60% data breaches has occurred in database which is migrated to the cloud, the organization has to allocate resource to strengthen application program interface (API) security measure by determining the probability of this specific threat. Several studies are conducted on the utilization of different networks including Bayesian; they have graphical models to show the dependencies among different variables in the cloud, for risk assessment to show the complicated links between the threats and the employed mitigation strategies. Usually, the determination of vulnerabilities during the development life cycle reduces the risk of exploitation in the production stage [18]. Queuing theory is used too for mitigation strategies analysing by understanding the behaviour of cloud resource under different workload environment. It also studies the effectiveness of cloud application in health care sector and improves resource allocation processes to overcome on the impact of the security threat. Furthermore, it helps to assess the performance of the cloud in response to the security threats [19]. The utilization of mathematical models greatly enhances the effectiveness of cloud security measure.

- **Mathematical Models in Cloud Security**

1. *Probabilistic Risk Assessment (PRA): -*

It evaluates the effectiveness of identifying and mitigating security threats.

$$=\frac{Number\ of\ Identified\ Threats}{Total\ Number\ of\ Threats} * 100\%$$

$$\text{PRA Score=}\ \frac{20}{30} * 100\% = 66.6$$

2. Queuing Theory Analysis:

It analyses cloud resource behaviour under workload conditions.

$$=\frac{Number\ of\ Improved\ Processes}{\text{Total Number of Processes}} * 100\%$$

$$\text{Queuing Theory Effectiveness} = \frac{8}{10} * 100\% = 80\%$$

3. Bayesian Network Analysis:

It identifies dependencies between variables in cloud environments

$$=\frac{Number\ of\ Accurate\ Predictions}{\text{Total Number of Predictions}} * 100\%$$

$$\text{Bayesian Network Score} = \frac{40}{50} * 100\% = 80\%$$

5. The Main Components of Cloud Computing

Clients:

They are all end users, who are using devices (Desktop, Lab top, iPods, Mobile) to access the data centers and all clients use all services and assets of the cloud computing. The main job of the client is to provide path to the resources by using web browser of the internet (Google, Firefox, Chrome). Client does not need advanced tools to access the resources of the cloud. Client components usually includes Graphical user interface to communicate with cloud infrastructure that provide services to the client. The service could be any software or platform that client may wish to implement.

Data Centers:

They are considered as a centre of all resources and they are used to store data and information on physical machines situated in different locations by cloud service providers that are required to be accessed.

Distributed Servers:

They always contain the applications which are used by the clients and are hosted by different numbers of servers. Since the services that offered by cloud are not limited in specific area so it has to be distributed in different servers which are located in different places [4]. All the distributed servers can be accessed through the internet. Multiple virtual machines can run on single host (physical server). The number of virtual machines will be limited according to the application type and size of physical server. Fig (1) shows the general connection of cloud configuration [3].

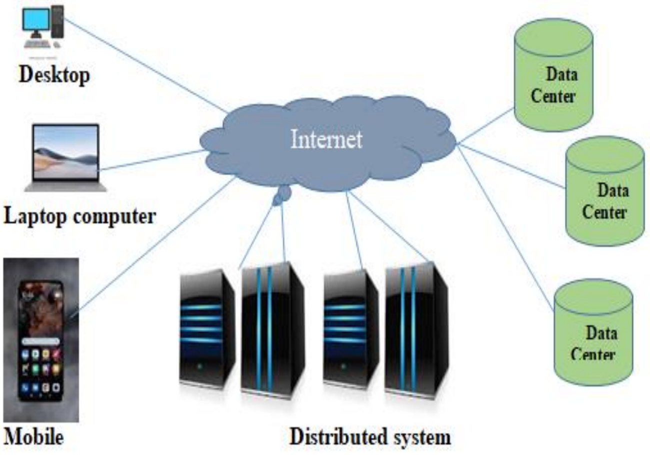


Figure 1: General Connection of Cloud Configuration

6. Types of Cloud Computing Services:

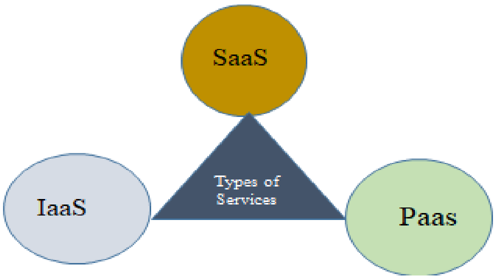


Figure 2: Cloud Computing Services

6.1 Software as a Service (SaaS)

Software as a Service (SaaS) is a type of cloud service that is held and hosted all applications software by provider and makes them available to all customers through the internet. All types of accessing can be achieved by web browser. Customers have to pay the fee for their subscription.. It can be accessed from different locations easily besides it can be customized and scaled up, Furthermore it neither needs extra hardware nor initial set up to run this type of service. The main problems of SaaS are to loss control and connectivity due to a certain circumstances that might happen accidently. Some examples for SaaS applications are project management tools and email service [4]

6.2 Infrastructure as a Service (IaaS)

In this type of cloud computing service the provider offers virtualized computing Software as a Service (SaaS) is a cloud-based service where a provider hosts and manages all applications software, making them accessible to consumers over the internet. Web browsers may be used to access many forms of information. Customers are required to remit the cost for their subscription. This sort of service is readily accessible from many places and can be customized and scaled up. Additionally, it does not need any additional hardware or initial setup to function. The primary challenges associated with SaaS are the potential loss of control and connection disruptions that may occur inadvertently due to unforeseen circumstances. In this type of cloud computing service, the provider offers resources such as storage, servers and networking to the users over the internet. The users can build their own applications by using these resources and deploy them with the services. The customers can do all management and maintenance of software application, which they are run on virtual infrastructure. The IaaS features are dynamic and flexible, easy to use because of automated deployment hardware, and due to the virtualized management, employees have more time to perform other task. But some difficulties may face the customers due to multi-tenant architecture in addition to the knowledge and training required for the new infrastructure. Finally customer can access the data only when venders are available in framework [5].

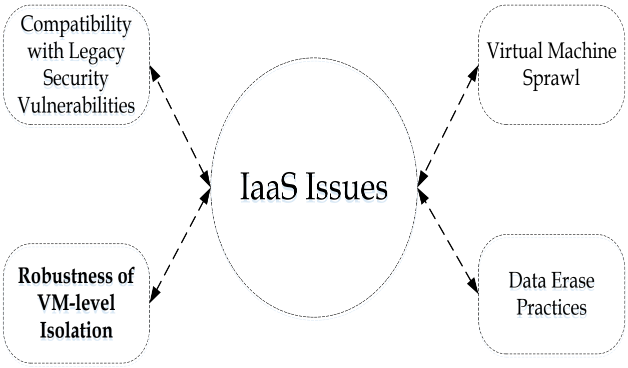

Compatibility with Legacy Security Vulnerabilities
Virtual Machine Sprawl
IaaS Issues
Robustness of VM-level Isolation
Data Erase Practices

Figure 3: Iaas Issues

virtualized computing resources such as storage, servers and networking to the users over the internet. The users can build their own applications by using these resources and deploy them with the services. The customers can do all management and maintenance of software application, which they are run on virtual infrastructure. The IaaS features are dynamic and flexible, easy to use because of automated deployment hardware, and due to the virtualized management, employees have more time to perform other task. But some difficulties may face the customers due to multi-tenant architecture in addition to the knowledge and training required for the new infrastructure. Finally, customer can access the data only when venders are available in

6.3 Platform as a Service (PaaS)

In this type of The Platform as a Service (PaaS) is a computing service that may be seen as an intermediary between Software as a Service (SaaS) and Infrastructure as a Service (IaaS). PaaS offers more flexibility and control compared to SaaS. PaaS providers provide services and tools to assist users in building and deploying applications, while also providing access to a platform for managing the underlying infrastructure. The applications are designed and validated with little cost. Additionally, the development process is expedited and

located on organization's premises or could be hosted on third party premises to provide the services. Public Clouds: These types of clouds are offering services to the public users but are not owned by them. Data centres are located in different places and may not necessary on the premises of users**.** They usually build by using IT infrastructure. For examples Amazon Web service (AWS), Google Cloud and IBM Cloud [7]. Required coding [6]. The IaaS allows moving toward hybrid cloud easily. The main problems for PaaS are the compatibility of the existing infrastructure and the data security

7. Main Types of Cloud Computing Systems

Private clouds: In this type of the cloud computing, it is used only for institutes, organizations and enterprises that need to keep their activities in safe with control and high security level. All computing resource such as servers, storage and network facilities are provided as a service to the users inside the organization. All private in this type of the cloud computing, it is used only for institutes, organizations and enterprises that need to keep their activities in safe with control and high security level.

framework [5].

streamlined, resulting in a decreased workload.

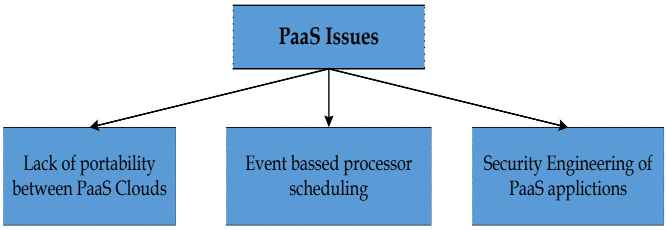
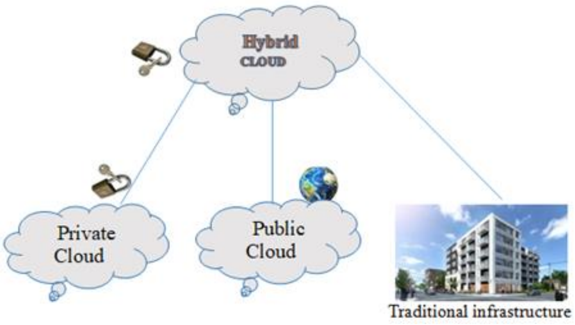

PaaS Issues
Lack of portability between PaaS Clouds
Event bassed processor scheduling
Security Engineering of PaaS applictions

Figure 4: PaaS Issue

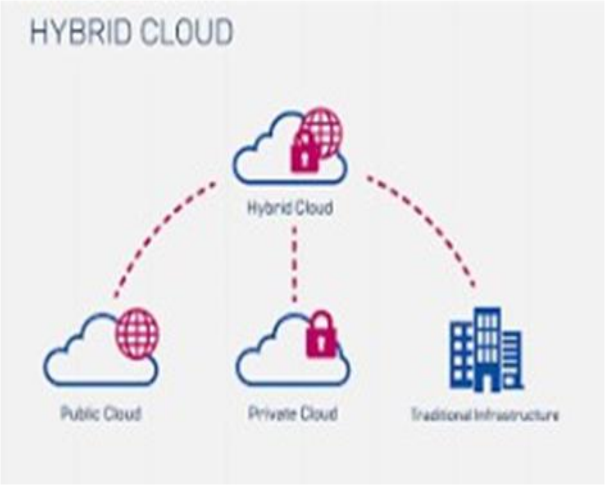
All computing resource such as servers, storage and network facilities are provided as a service to the users inside the organization. All private cloud computing equipment and data center are

issues in addition to the reliability and the support which depend on the vendor's speed efforts Fig. (5) shows cloud computing services.

Hybrid Clouds: This type of cloud has complex characteristics and different requirements applied to put it in operation. It consisted of several computing environments that combines an on-premises datacenter (private cloud) with a public cloud, allowing data and applications to be shared between them by using LANs, WANs, and APIs to form single unified environment [8].



(a)



(b)

Figure (5 a-b) Types of the cloud computing

multi-clouds This type consisted of multiple cloud services from private and public clouds venders. When multiple clouds link together, they become hybrid type but not all multiple clouds are hybrid clouds but all hybrid clouds are multiple clouds [9].

Board network access in order to let maximum number of people can access the cloud computing services, there must be reliable broad network access. Clients can access the network through personal computer, tablets, laptops and mobile phones. All audience can make use of this technology.

Resource pooling: Since Cloud Computing are used to offer service to many people at the same time, that means the available physical and virtual resources (storage, memory, processing and network facilities) have to be shared among multiple customers which are dynamically assigned and reassigned resources according to the customer demand [10]. The actual required data location is unknown for the customers and stored at provided resource. General public people Developer Community Model It refers to specific group of customers that get services of cloud computing for various purposes, and all resources are offered by the cloud computing are dedicated to this specific particular group only.

8. The Characteristics of Cloud Computing

On Demand Self –Service: It means the client can access the resources at any time and cloud computing can provide services on request without interaction of the service provider or any human being. The capabilities that include server time and network storage can be supplied to the customers automatically.

The public people Developer concept gives the opportunity to the people (who cannot code) to code. By using the proper tools, the ordinary folks (those of us that has no specialty in computer science) can have access to the application program interfaces APIs and create customized automation [11]. In year 2023 Google, AWS, Microsoft, and other companies have created tools for developers to build complicated applications with drag and drop interface easily. Microsoft's Power Platform is the leader in the Power AI, Power flow, Power Builder, and Power Apps. The complex mobile trends and Web applications can be created by using the four combined tools to interact with the business tools. The competition among AWS, Microsoft and Google Cloud Platform have been taking the first trends since year 2023. The competition has taken in consideration the following factors: -

- The Cost and Pricing.
- All Incentives parameters
- Performance and Reliability
- Other related factors

Decreasing the cost is the main factor to avoid the investment barriers. The AWS model applies that the payment depends on the usage (you pay for what you use). This will be implemented in all services. This will cut short the subscription models and replace it. Expect

* Corresponding author E-mail address: drmohammednofa@gmail.com

https://doi.org/10.61268/gmqmnm28

that all cloud companies deliver tools to show resource usage and the service's per-byte cost [12].

- Common Threats to Cloud Computing Security

Since cloud computing based on platform technology, numerous prevalent threats may attack it. There are many types of threats, data breaches are one of them which is perpetrated by unauthorized people. The data breaches or data theft of an organization’s private information may cause a lot of damages to the reputation and finance of the organization itself. In this case strict security measures must be taken to protect the data. Malware attacks are widespread too, can hack the cloud server and steal the data. In such cases machine learning is used to secure their data. Some suspicious activities are used to compromise email account and impersonate a person, which are committed by hackers. To avoid this type of attacks, encryption of data and information is used by applying different ciphering algorithms. Another type of attack is distributed denial of service (DDoS) which is used to disrupt the regular working of company’s system and organizations.

9. Security Strategies and it’s mitigation in cloud computing

There are different methods to ensure the security of cloud computing. The most prevalent significant one is the encryption method. Encryption techniques have been used to convert data and information into unreadable format, which can be read only by authorized people by using decryption key only. Data Encryption Standard (DES) is a block ciphering method of size 64 alphabet characters. It is widely utilised to protect the data. Another method of ciphering, RSA is an asymmetric cryptography algorithm which works on two different keys. **Public Key** and **Private Key.** The Public Key is given to everyone and the Private key is kept private. These encryption techniques have been utilized to secure data storage in addition to their highly effective in ensuring cloud security the effectiveness of encryption in preserving data integrity can be expressed as follows: -

$$Data\ integrity = \frac{Number\ of\ decrypted\ messages}{Total\ \ number\ of\ encrypted\ message}$$

- **Identity and Access Management (IAM):**

IAM is utilized to control the access of the services and resources of the cloud computing. Only authorized user can access private information. The identity access management can be measured by the following equation:

$$IAM = \frac{Number\ of\ authorized\ access\ request}{Total\ Number\ \ of\ access\ \ requests}$$

- **Security information and events management** (SIEM):

This type of strategy has been utilized to protect the data by analysing the data of the security event by using the available resources in the cloud computing. This will help to get more information about the security problem of the organization or company. The SIEM can be measured by the following formula.

$$\textbf{SIEM} \ = \frac{\boldsymbol{Number\ of\ Detected\ threat}}{\boldsymbol{Total\ number\ of\ threts}}$$

Another technique can be used to mitigate the security vulnerabilities in cloud computing which depends on the management of the vulnerabilities.

10. Cloud Computing Challenges

Cloud computing faces many challenges, that includes security problems, compliance, control of governance, internet connectivity, lack of expertise, in addition to many other problems as explained below [14]:

Visibility into cloud data Cloud services cloud be accessed from outside of corporate network or from devices not under the control of IT, which is opposed to traditional means of monitoring network traffic.

Data Privacy: Data privacy is another major challenge in cloud computing. Businesses need to ensure that their data is stored and processed in compliance with data privacy regulations such as GDPR (General Data Protection Regulation which governs how the personal data of individuals in the EU may be processed and transferred) [15]. Portability: One of the problems that faces cloud computing is transfer applications from a certain provider to another because each cloud provider uses different standard language for their platform. Hopefully this problem could be solved by collaboration among the cloud providers in the near future.

Compatibility and Interoperability: It means the application on certain Platform could incorporate service from other different platform by using another Web service which is hard to develop, that leads to a new challenge to the cloud computing. Reliability and availability: Many people are used to store data and useful information in cloud computing in order to access them easily at any time and from anywhere. So, the cloud has to be robust and reliable because most of the businesses depend on the services that are provided by the third party.

The efficiency of cloud computing is determined by the performance of the cloud services offered to customers. In order to ensure optimal performance, it is essential to meticulously address and eliminate any obstructions that hinder efficiency on the platform. Cost Management: Cloud computing may incur significant expenses, and firms must diligently oversee their expenditures to prevent unforeseen financial obligations. Successful implementation of this task requires meticulous strategizing and financial allocation, as well as vigilant oversight and enhancement of utilization [16].

Integration: The process of incorporating cloud services into an organization's current IT infrastructure is a significant obstacle. Businesses must verify the compatibility and smooth integration of their cloud solutions with their current systems and applications. Vendor Lock-In: Businesses must be cognizant of the potential for vendor lock-in when selecting a cloud provider. This may restrict their adaptability and provide challenges in transitioning to other service providers in the future.

11. Benefits of Cloud Computing

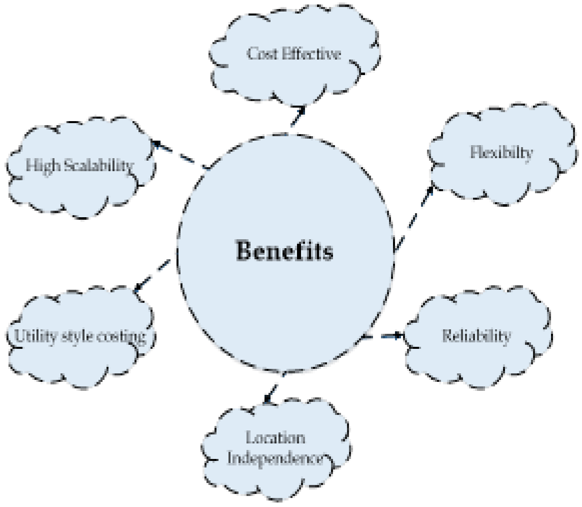


Figure 6: Benefits of cloud computing

Cost Savings: Cloud computing offers a more economical solution compared to on-premises infrastructure since customers are only charged for the specific resources they use [17]. Scalability: Cloud computing allows customers to rapidly and effortlessly adjust the size of their operations according to their requirements. This allows us to promptly adapt to fluctuating market circumstances and meet the evolving expectations of our customers. Cloud computing provides organizations with more flexibility in terms of their work location and methods. Employees have the ability to remotely access programmers and data from any location with an internet connection, facilitating remote work and collaboration.

Disaster Recovery: Cloud computing enables firms to swiftly recover from disturbances, such as natural catastrophes or cyber-attacks. Cloud providers provide disaster recovery solutions that guarantee uninterrupted company operations in the case of an interruption. Cloud computing facilitates rapid innovation for companies by providing access to novel technology and services.

Cloud providers consistently provide novel functionalities and capacities to enable enterprises to maintain competitiveness and adapt to market developments.

Essential attributes of cloud computing The National Institute of Standards and Technology (NIST) defines cloud computing as a model where users pay for the use of computing resources such as networks, servers, storage, applications, and services. These resources are easily accessible through a network and can be quickly provided and released with minimal effort or interaction with the service provider. The essential attributes that a cloud should possess are:

- pay-per-use (no ongoing commitment, utility prices);
- Elastic capacity and the illusion of infinite resources;
- Self-service interface; and Resources that are abstracted or virtualized.
- The elimination of an up-front
- commitment by cloud users;

Protection and durability of cloud-based systems The data saved in the cloud is encrypted while it is at rest, which ensures that it is safe from unauthorised access, even while it is kept on servers. Encryption functions as a safeguard, making critical information incomprehensible to unauthorised individuals or possible dangers. Encryption is used to maintain the secrecy of data as it moves between the user's device and the cloud servers. This helps to reduce the chances of unauthorised interception by malevolent individuals. Contemporary cloud systems use cutting-edge encryption methods, such as Advanced Encryption Standard (AES), to maintain the utmost level of secrecy.

With the increasing migration of enterprises to the cloud, ensuring security and resilience has become paramount. Cloud companies are making significant investments in security and resilience measures to safeguard customers' data. Cloud companies prioritise investing in features such as data encryption, access restrictions, and disaster recovery to guarantee the protection of their customers' data. Businesses that are transitioning their activities to the cloud have a significant apprehension over security. Due to the vast scale of the network in cloud computing, ensuring a high degree of security and privacy for each client is challenging. Cyber-attacks pose a significant threat to the security of cloud systems. The primary concern is the potential for data leakage, which may be mitigated by the use of robust security measures such as encryption methods and hardware safeguards. security equipment in addition to the security application for data protection.

Cloud security includes all the technical measures and procedures to protect cloud computing environment against both internal and external cyber-attack threats. The security responsibility is the first step to building a cloud security strategy. Cloud computing is used to deliver information technology over the internet for businesses and governments, which needs security to prevent unauthorized access to the network and avoid all vulnerabilities in the system. By applying cloud security, all applications and information will be secured from all types of attacks. Since there are four categories of cloud computing as shown in Fig. (6), so the Cloud security differs based on the category of cloud computing being used. Cloud security responsibilities are taken by most cloud providers to create a secure cloud and maintaining public and customer trusts.

- Public cloud services, operated by a public cloud provider, data and applications are hosted with a third party.
- Private cloud services, dedicated to one customer operated by a third party.
- Private cloud services, operated by internal staff — These services are an evolution of the traditional data center.
- Hybrid cloud services — Private and

public cloud computing is combined to optimize factors such as cost, security, operations and access. Operation will involve internal staff, and optionally the public cloud provider.

12. Types of cloud security responsibilities

The cloud provider and cloud customer share different levels of responsibility for security. By service type, these are [19]: Software-as-a-service (SaaS) — Customers are responsible for securing their data and user access. Platform-as-a-service (PaaS) — Customers are responsible for securing their data, user access, and applications. Infrastructure-as-a-service (IaaS) — Customers are responsible for securing their data, user access, applications, operating systems, and virtual network traffic. Customers are responsible for securing their data and controlling who can access that data. within all types of public cloud services. Data security in cloud computing is important issue to successfully use and gain the benefits of the cloud computing. Organizations like Microsoft Office 365 or Salesforce, they are cobrated together to share responsibilities to protect data in the cloud computing.

13. Conclusion

Cloud computing technology has the benefit of simplifying data management, but users must exercise caution and be vigilant on the associated security risks and problems. Various strategies may be used to address security concerns, including the implementation of a shared responsibility model and the utilization of new technologies to reduce cloud security risks and enhance the resilience of security systems in a cloud environment. Other significant forms are serverless computing and containerization. These categories significantly influence the level of risk associated with vulnerabilities and misconfigurations. Which individuals may exploit. Comprehending the potential hazards and new technologies is vital while implementing conventional security protocols. In order to prevent user errors, it is necessary for individuals to cultivate a feeling of responsibility towards their customers via e-learning or attending relevant courses.

This article explores the development of cloud computing and provides a detailed explanation of the key features of the four main models: private, public, hybrid, and community. Cloud service providers provide high availability, ensuring that their infrastructure and services are consistently available as required. Cloud computing may obviate the need of purchasing and upkeeping resources or equipment on the premises. Utilizing cloud technology allows for a more efficient and expedient access to resources. Individuals and corporations may get the necessary resources at any given time. It is mostly associated with the advancement of information technology and the management of data.

Cloud computing is a rapidly growing technology that has been extensively adopted by many organizations, institutions, and individuals. It provides several benefits for entrepreneurs. Transparency is a crucial limitation in any cloud computing framework, along with security, scalability, and intelligent monitoring. The extra constraints facilitate the development of novel functionalities to enhance the complexity of the cloud computing infrastructure. It facilitates the optimization of operations, expedites innovation, reduces expenses, and also adds to long-term growth improvement. The pros and drawbacks of cloud computing services, including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), are explained. An issue arises when there is a flawed setup of cloud computing, which may result in significant financial losses that are ten times higher compared to the expected performance of the standard objective. The cost savings from cloud architecture are much higher for operations that often perform comparable tasks. Choosing a cloud setup that can simultaneously meet several needs, such as high accuracy, little overhead, and flexibility for multiple applications, is a challenging task. Although there are obstacles, there are significant advantages associated with the cost savings, scalability, and superior performance of cloud computing via the internet. Prior to embarking on the transition to cloud computing, the organization should thoroughly evaluate the advantages of cloud services, including cost reduction, adaptability, expandability, and dependability, in order to address potential challenges associated with cloud computing.

References

[1] R. Islam et al., ‘The Future of Cloud Computing: Benefits and Challenges’, Int. J. Commun. Netw. Syst. Sci., vol. 16, no. 4, pp. 53–65, 2023.

[2] J. Ahola, ‘Cloud monitoring: cloud monitoring with dynatrace’, 2022.

[3] M. Sharma, R. Gupta, and P. Acharya, ‘Analysing the adoption of cloud computing service: A systematic literature review’, Glob. Knowledge, Mem. Commun., vol. 70, no. 1/2, pp. 114–153, 2021.

[4] M. U. Saleem et al., ‘Integrating smart energy management system with internet of things and cloud computing for efficient demand side management in smart grids’, Energies, vol. 16, no. 12, p. 4835, 2023.

[5] V. A. Thiviyanathan, H. R. Lim, P. E. Tham, and P. L. Show, ‘How far has the development for industrial Internet of Things (IoT) in microalgae?’, in Microalgae for Environmental Biotechnology, CRC Press, 2022, pp. 145–174.

[6] B. Benmammar and A. Amraoui, ‘Artificial Intelligence Application to Cognitive Radio Networks’, Intell. Netw. Manag. Control Intell. Secur. Multi-criteria Optim. Cloud Comput. Internet Veh. Intell. Radio, pp. 217–243, 2021.

[7] D. Nikhil, B. Dhanalaxmi, and K. S. Reddy, ‘The evolution of cloud computing and its contribution with big data analytics’, in Innovative Data Communication Technologies and Application: ICIDCA 2019, 2020, pp. 332–341.

[8] H. Tschopp, ‘Future Trends in Finance, Software, and Technology’, 2023.

[9] R. Sivan and Z. A. Zukarnain, ‘Security and privacy in cloud-based e-health system’, Symmetry (Basel)., vol. 13, no. 5, p. 742, 2021.

[10] F. P. Appio, F. Frattini, A. M. Petruzzelli, and P. Neirotti, ‘Digital transformation and innovation management: A synthesis of existing research and an agenda for future studies’, J. Prod. Innov. Manag., vol. 38, no. 1, pp. 4–20, 2021.

[11] X. Jin, W. Hua, Z. Wang, and Y. Chen, ‘A survey of research on computation offloading in mobile cloud computing’, Wirel. Networks, vol. 28, no. 4, pp. 1563–1585, 2022.

[12] T. Wang, Y. Liang, X. Shen, X. Zheng, A. Mahmood, and Q. Z. Sheng, ‘Edge Computing and Sensor-Cloud: Overview, Solutions, and Directions’, ACM Comput. Surv., 2023.

[13] S. H. Murad and K. H. Rahouma, ‘Implementation and performance analysis of hybrid cryptographic schemes applied in cloud computing environment’, Procedia Comput. Sci., vol. 194, pp. 165–172, 2021.

[14] A. Katal, S. Dahiya, and T. Choudhury, ‘Energy efficiency in cloud computing data centers: a survey on software technologies’, Cluster Comput., vol. 26, no. 3, pp. 1845–1875, 2023.

[15] F. K. Parast, C. Sindhav, S. Nikam, H. I. Yekta, K. B. Kent, and S. Hakak, ‘Cloud computing security: A survey of service-based models’, Comput. Secur., vol. 114, p. 102580, 2022.

[16] H. Tabrizchi and M. Kuchaki Rafsanjani, ‘A survey on security challenges in cloud computing: issues, threats, and solutions’, J. Supercomput., vol. 76, no. 12, pp. 9493–9532, 2020.

[17] M. J. Khan et al., ‘Identifying Challenges for Clients in Adopting Sustainable Public Cloud Computing’, Sustainability, vol. 14, no. 16, p. 9809, 2022.

[18] Y. Zhang, R. H. Deng, S. Xu, J. Sun, Q. Li, and D. Zheng, ‘Attribute-based encryption for cloud computing access control: A survey’, ACM Comput. Surv., vol. 53, no. 4, pp. 1–41, 2020.

[19] M. Sharma, R. Kumar, and A. Jain, ‘Load balancing in cloud computing environment: A broad perspective’, in Intelligent Data Communication Technologies and Internet of Things: Proceedings of ICICI 2020, 2021, pp. 535–551.