Cybersecurity Guidelines for cloud computing

Training Content for Teachers

Trainer's Booklet

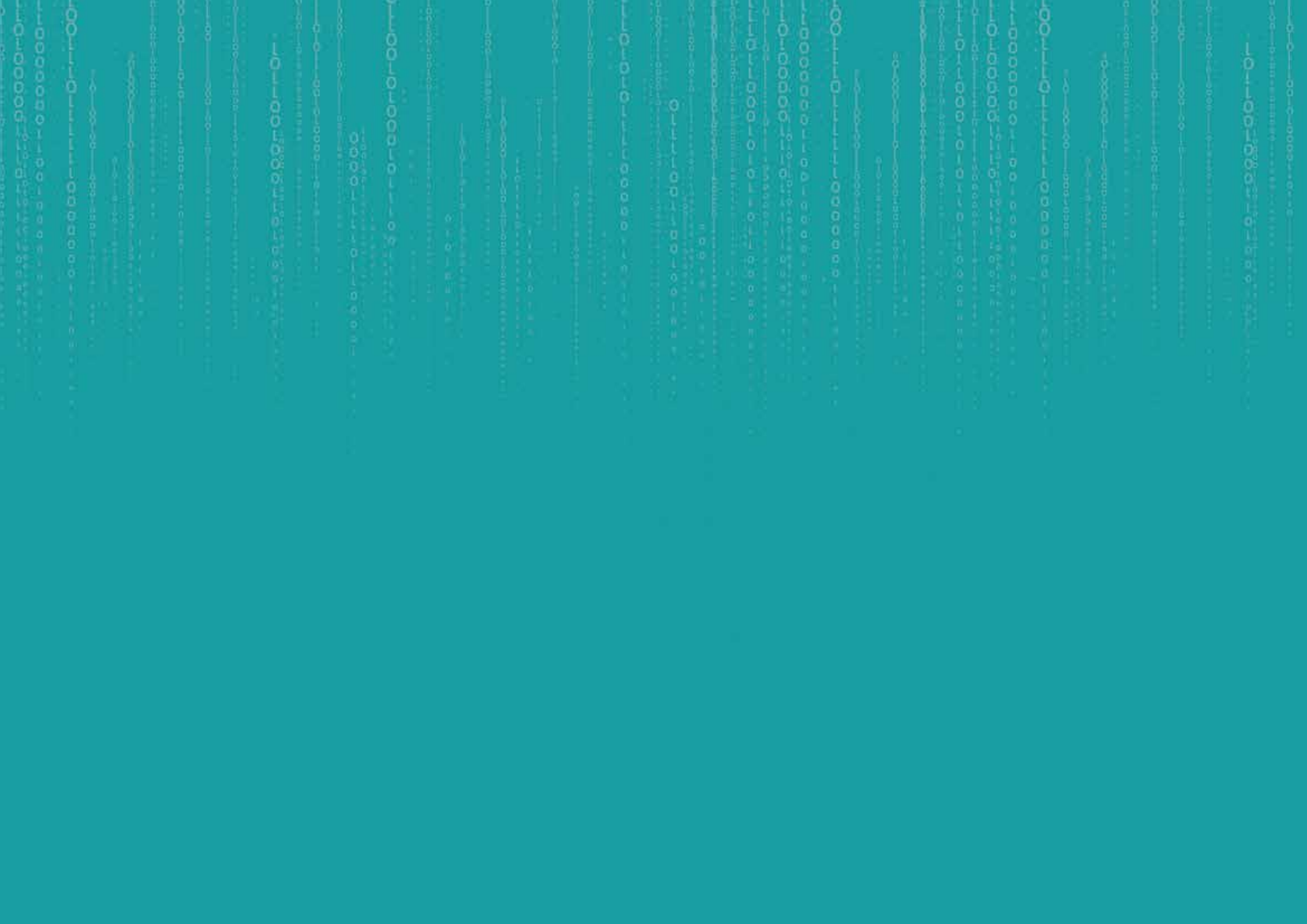
CyberEco

معًا لدعم السلامة الرقمية

Together to support digital safety

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency



Cybersecurity Controls for Cloud Computing

Training content for teachers

Training Kit

Trainer's Booklet

Intellectual Property rights

December, 2023

Doha, Qatar

This content is produced by the team of

National Cybersecurity Excellence Management, National Cyber Security Agency.

For inquiries about the initiative or program, you can contact us through the following websites or phone numbers:

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

https://www.ncsa.gov.qa/

cyberexcellence@ncsa.gov.qa

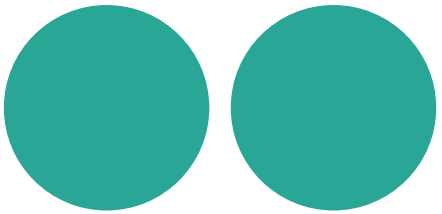
00974 404 663 78

00974 404 663 62

General content of the Kit

First: General Introduction to the training kit

Second: Scientific content



First: General Introduction to the Training Kit

Below is an explanation of some details relevant to the objectives of the training kit, along with general guidelines for the trainer on how to handle this kit, while providing him with the scientific content that will be relied upon during the training.

General Idea

The concept of this training kit is to equip the trainer with tools and training resources, making it easier for him to deliver information to the trainees. In general, each training material consists of two parts: One part for the trainee and another for the trainer. The training kit serves as a general guide and support for the trainer, and its scientific content is the same as that of the trainee, but here the training content is presented differently. Additionally, the kit equips the trainer with training tools and methods that support him in the training process.

Objectives of the Training Kit

- Providing the trainer with training tools that help him deliver the training content to the Trainees.
- To present information and training content in an easy and simple manner.
- To offer training content on protection of electronic devices along with multiple training tools and methods.

Contents of the Training Kit

The training kit includes several training tools, as detailed below:

1. **Presentation files.**
2. **Educational videos.**
3. **Training cards,** comprising general information accompanied by illustrative images,the trainer presents it to the trainees.
4. **Sketches,** including information about the main topics in the training content.

Content of the Training Kit

WorkShop Timetable

Content	Allocated Time
General introduction	15 minutes
The theoretical aspect	45 minutes
Educational Videos	25 minutes
Short break	20 minutes
Dialogue and discussion with trainees	15 minutes
Total training time	2 hours

Trainer's Guidance Manual

The following is an explanation of some general guidelines for the trainer, revolving around how to use this training kit:

1. The scientific content may include concepts beyond the trainers' expertise, so the trainer must present the information in a simplified manner.
2. The trainer presents slides for each point discussed. For example, when talking about the concept of cloud computing. The slide discussing this topic is being presented
3. The trainer displays the part related to **"Sketches"** in the end of the lecture
4. During the presentation of the scientific material for each chapter, a portion of the allocated time is used to present several links related to the content of the chapter.
5. Please open discussion with trainees in the places the trainer deems appropriate.

Second: Scientific Content

Introduction

In the current digital explosion in our world, we are all exposed to various newly-coined terms. One such term is cloud computing, a concept that has gained significant prevalence in recent years. Whether among experts in the technical domain or individuals without specialized knowledge, cloud computing has evolved into a vital technology used on a daily basis.

Cloud computing designates the location where data is stored, accessed, and processed over the internet. This location is commonly referred to as a 'server' in computer terminology. To put it differently, cloud computing is a technology that provides a range of services, encompassing data storage, computing resources like servers, databases, various software, and data processing and analysis.

Numerous global enterprises offer cloud computing services, including SkyDrive. These services focus on cloud storage using Microsoft servers after the user creates a personal account within the company's domain. Currently, this service is known as OneDrive.

Alongside Microsoft's services, the global company Google also offers cloud computing services. One of the most widely used cloud storage services is Google Drive Storage. Some of these services are available for free, while others require a subscription fee. They enable users to store their files from any device at any given moment. Nonetheless, an internet connection is essential for convenient access, retrieval, and interaction with files.

Chapter One

The Concept of Cloud Computing

- The importance of cloud computing.
- Types of cloud computing.
- Challenges of Cloud Computing.

01

The importance of cloud computing

Cloud computing refers to accessing a range of services, including tools and applications such as data storage, servers, databases, networks, and software, over the internet. Instead of storing files on your local hard drive or private drive, you can store documents in a database on the network using the cloud. So long as your electronic devices have an internet connection, you can access the data and software needed to run them.

The importance of cloud computing can be attributed to several reasons, with cost savings and increased productivity being the most prominent advantages. Other benefits include enhanced speed, efficiency, and security. Cloud computing provides a diverse range of services over the internet, including data storage, servers, databases, networks, and software. It is becoming increasingly prevalent among individuals and businesses seeking more storage space for their data. It serves as an effective solution for off-site data backup [1].

Cloud-based storage enables you to store files in a remote database and retrieve them whenever required. These services can be either public or private. Public services are offered over the internet for a fee, while private services are hosted on the network for specific clients.

As for the reason behind naming it 'cloud computing,' it is because the information accessed is remotely stored in the cloud or virtual space. Companies that offer cloud services enable users to store files and applications on remote servers, allowing access to all data over the internet. It is a general term used by professionals in the technology industry to describe these servers and network infrastructure. Users do not need to be in a specific location to access them[2].

1. Frankenfield, Jake. What is Cloud Computing? Pros and Cons of Different Types of Services, investopedia, April 2023. On site: https://www.investopedia.com/terms/c/cloud-computing.asp
2. Weinberger, Matt. Why 'cloud computing' is called 'cloud computing', businessinsider, Mar 2015. On site: https://www.businessinsider.in/why-cloud-computing-is-called-cloud-computing/article-show/46544750.cmsshow/46544750.cms

Cloud computing bears all the heavy burdens associated with data processing away from the device you carry or work on.It transfers all this work to massive computer clusters located remotely in the digital realm. In this way, the internet becomes like a cloud, making your data, work, and applications accessible from any device that allows you to connect to the internet from anywhere in the world.

Overall, the importance of cloud computing is evident through the following points:

1. Cost savings

In the long term, cloud computing services offer a chance to save money and, as a result, the possibility to invest in other business-related areas. Most cloud services operate on a pay-as-you-go basis, meaning there is no scope for squandering funds on services that won't be used.

One of the aspects in which cloud computing enables cost savings is in the acquisition of costly hardware and software. This implies no further maintenance for local servers, as users can store their data on the chosen cloud services provided by companies offering this type of technological service.

2. A reliable and secure environment

Cloud computing is deemed more secure and reliable than local systems. As cloud service providers employ teams of experts who manage the infrastructure and ensure smooth operations. This enables users of these services to concentrate on their work, even during emergencies such as power outages and natural disasters like fires. These servers safeguard user data.

3. Cooperation

Some companies encounter challenges when trying to access data within their systems, leading to time and financial losses. This has created a demand for offsite (remote) data storage, a service provided by cloud computing companies that include teams of specialists and technicians working to ensure data security on servers. Consequently, they promote smooth collaboration among teams, saving time and enhancing cooperation among employees, whether within the company's premises or from various locations around the world.

4. Developability

Cloud computing is characterised by its flexibility and complete developability according to business needs. Users can expand or reduce their cloud capacity based on their personal and operational requirements.[1].

1. Linao, Portia. Why is it called "The Cloud"? officesolutionsit, February 2023. On site: https://www.officesolutionsit.com.au/blog/why-is-it-called-the-cloud

Types of cloud computing

Cloud service providers employ advanced security technologies, including encryption, firewalls, and access restrictions, to safeguard data from unauthorized access. It ensures the preservation of information even if your nearby devices are damaged or stolen.

Generally, there are several types of cloud computing; below is an explanation of the most important ones:

Public cloud:

It is open and available to everyone to store and access information online using the pay-as-you-go model. The compute resources are managed and operated by a cloud service provider who takes care of the supporting infrastructure and ensures that resources are available and scalable for users. Anyone with an internet connection may use the public cloud irrespective of their location or company size to store their data and run applications. Examples of this include: Amazon Elastic Compute Cloud (EC2), IBM SmartCloud Enterprise, Microsoft, Google App Engine, and Windows Azure Services Platform.

Public cloud computing is characterised by several features, including:

1. **Ease of access:** Cloud computing is available to everyone with an internet connection, and users can access their data and applications from anywhere at any time.
2. **Common infrastructure:** Many users share infrastructure in public cloud settings, which has helped to reduce costs.
3. **Scalability**: Users can easily adjust the resources they need based on their requirements, allowing them to scale up or down as they wish.
4. **pay-as-you-go:** In the public cloud, payment is based on usage only, that is, in exchange for the resources that the user actually uses, which reduces costs.

5. **Ease of maintenance and administration:** As public cloud computing is managed by service providers, they are responsible for managing and maintaining the infrastructure. They manage hardware maintenance, software updates, and security tasks more efficiently and without any involvement from users.(1)

Disadvantages of public cloud computing:

Public cloud computing has a number of disadvantages, **as follows:**

- Public cloud storage is less secure than other storage media because the data and information stored is publicly accessible.
- The effectiveness of cloud computing is directly linked to the quality and speed of internet service. Any disruption or impairment in internet networks will have a direct impact on the performance of cloud computing and the capacity to access data stored therein.
- Users have a relatively limited degree of control over the data stored in the cloud.
- Concerns about data privacy and confidentiality.
- The possibility of users incurring unexpected additional costs if there are changes to the terms of use.
- The absence of customisation alternatives and flexibility in comparison to private or hybrid cloud environments (Γ).

1. Stephen J. Bigelow. What is public cloud? Everything you need to know, techtarget. On site: https://www.techtarget.com/searchcloudcomputing/definition/public-cloud
2. Types of Cloud, javatpoint. On site: https://www.javatpoint.com/types-of-cloud

2. Private cloud computing

Private cloud computing is also known as an internal cloud or corporate cloud, and is employed by enterprises to create and manage their private data centres, either in-house or through external service providers. Examples consist of:

- VMware vSphere, OpenStack, Microsoft Azure Stack, Oracle Cloud at Customer, and IBM Cloud Private.

Private cloud computing is categorised into two forms:

Private cloud computing within the enterprise: This entails a private cloud integrated within the physical infrastructure of the enterprise, which comprises the creation and operation of a designated data centre that offers cloud services solely for internal use within the company. Hence, the complete infrastructure remains under the control of the enterprise's management, providing them with the liberty to modify and configure it in a manner that they consider suitable. In this form, the enterprise can manage security concerns.

Nevertheless, the opposite aspect of this form of private cloud is that it necessitates significant expenditures on hardware, software, and IT proficiency.

Private cloud computing that involves leveraging external resources: This pertains to leveraging external resources, such as collaborating with an external service provider to host and manage the cloud infrastructure on behalf of the enterprise. It is possible for the provider to operate the private cloud within their own data centre or in a shared facility. Consequently, the enterprise could profit from the knowledge and resources of the service provider, thus decreasing the load of infrastructure management. Furthermore, the external service provider can modify resources in accordance with the requirements of the enterprise.

This model is appealing to enterprises that wish to obtain the advantages of private cloud usage without incurring costs for maintenance, software, and hardware[1].

Private cloud computing offers numerous advantages:

1. It provides enterprises with increased control over their data, applications, and security.

1. What is private cloud? Types, process, benefits, examples, knowledgehut. On site: https://2u.pw/vtxJ57Q

2. It is particularly well-suited for enterprises with stringent compliance requirements, sensitive data, or specialised workloads that require high levels of customisation and security.
3. The exclusive leveraging of private cloud computing is allocated for a sole enterprise, thereby ascertaining that resources and services are customised to fulfil its needs.
4. It offers greater control and security compared to public cloud alternatives for enterprises.
5. Private cloud computing empowers enterprises to customise the infrastructure in accordance with their specified requirements.
6. Private cloud computing is scalable and permits enterprises to increase their resources in accordance with demand and customise them accordingly.
7. Private clouds provide enterprises with greater command over their infrastructure, thus augmenting both performance and reliability.
8. Enterprises can meet certain compliance and regulatory requirements more effortlessly by leveraging a private cloud. By provisioning the freedom to implement high-strength security protocols, adhere to data residency laws and comply with industry-specific regulations.
9. Private clouds may be integrated with public cloud services to create a hybrid cloud infrastructure, which enables enterprises to leverage the advantages of both private and public clouds[1].

Disadvantages of private cloud computing

1. Effective management and operation of cloud services necessitates a proficient workforce.

2. Private clouds can be accessed within the enterprise, thereby constraining the operational area.

3. Private clouds may not be suited for enterprises that have a vast user base and lack pre-existing infrastructure and sufficient workforce to ensure optimal maintenance and management of the cloud.

4. The elevated primary costs along with incessant maintenance expenditures.

1. What is private cloud? ovhcloud. On site: https://www.ovhcloud.com/en-gb/learn/what-is-private-cloud/

5. Increasing resources can pose a challenge when compared to public or hybrid cloud alternatives.

6. Internal IT personnel are dependent upon to manage, detect, and rectify issues.

7. Slower timelines for usage and implementation when compared to public cloud solutions.[1]

8. Restricted accessibility to the latest advancements and innovations rendered by public cloud service providers.

9. Lesser degree of flexibility and agility when compared to public cloud alternatives.

10. Difficulties in maintaining alignment with updates to hardware and software, as well as ensuring compatibility.

11. The necessity for periodic infrastructure updates.[2]

3. hybrid cloud:

This is a hybrid cloud computing that combines public and private cloud services. It is relatively secure because services running on the public cloud can be accessed by anyone, while services running on the private cloud can only be accessed by the enterprise's users.

In this type of clouds, enterprises can leverage the advantages of both public and private clouds to create a flexible and scalable computing environment. The public cloud component provides access to cloud services offered by third-party providers that can be utilized through the internet. A few examples of such services are:

- Google Application Suite (Gmail, Google Apps, and Google Drive), Office 365 (MS Office, OneDrive), and Amazon Web Services.

Hybrid cloud features:

Hybrid clouds offer several advantages, below is an explanation of the most important ones:

- The hybrid cloud operates by integrating both the public and private clouds, facilitating the utilization of both cloud types.
- It offers flexibility in resource allocation and scalability, through the utilization of supplementary resources from the public cloud, while preserving authority over essential workloads on the private cloud.

1. Public and Private Cloud Advantages and Disadvantages, connectria. On site: https://cutt.us/cMN8l
2. 6 Advantages and Disadvantages of Private Cloud | Limitations & Benefits of Private Cloud, hitechwhizz. On site: https://cutt.us/CplCr

- It functions to reinforce security and control, as it provides a secure and dedicated environment, while leveraging public cloud resources for non-sensitive tasks.
- Cost optimisation through the use of cost-effective public cloud for non-critical workloads, while retaining critical applications and data on the most cost-effective private cloud.
- The capability to transfer data and applications between public and private clouds as required.
- A hybrid cloud helps process compliance and regulatory requirements more efficiently, allowing sensitive data and applications to be retained within the private cloud while utilizing the public cloud for other non-sensitive operations.
- A hybrid cloud enables the facilitation of disaster recovery and business continuity by duplicating essential data and applications between the private and public cloud, ensuring redundancy and mitigating the risks of data loss or service interruption.[1]

Disadvantages of hybrid cloud:

- The security feature does not match the quality of the private cloud.
- Managing a hybrid cloud is complicated due to the challenge of running multiple usage models.
- The reliability of services is dependent on cloud providers.
- The growing challenges in data integration and the assurance of connectivity between diverse cloud platforms.
- Increased expenditures result from the necessity to manage and integrate various cloud environments.
- Increased intricacy in managing data across multiple cloud providers.
- Dependence on stable, high-bandwidth internet connections for effective hybrid cloud operations.
- Demands proficient IT personnel experienced in the management of hybrid cloud technology.

1. What is hybrid cloud? netapp. On site: https://cutt.us/8N9QZ

4. Community Cloud

The community cloud permits access to systems and services provided by consortium of multiple enterprises for the purpose of sharing information within the enterprise and a particular community. It is owned and managed by one or more enterprises within the community, a third party, or a consortium of them.[1]

In the configuration of the community cloud, collaborating enterprises, whether from the same industry, the public sector, or any other community, work together to create a common cloud infrastructure. This allows them access to services, applications, and shared data relevant to their respective community. Example: The healthcare community cloud.

Community Cloud advantages

1. The community cloud provides a shared infrastructure that can be accessed by a specific community of enterprises.
2. The community cloud provides resources, applications, and services that are customised to meet the needs of the participating enterprises. These services are created to meet the requirements while promoting effective communication and information exchange.
3. A community cloud may be owned and administered by one or more enterprises within the community, a third party, or a combination of both. Participating enterprises play a significant role in governance and decision-making to ensure that the cloud infrastructure aligns with their shared objectives.

1. Mohanakrishnan, Ramya. What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, spiceworks. On site: https://cutt.us/ORUiy

4. The community cloud adheres to security and compliance procedures relevant to a specific community. It allows for the implementation of robust security controls, access management, and compliance frameworks that meet the organizational requirements of the community and industry standards.
5. Participating enterprises in a community cloud benefit from the sharing of costs.
6. Community cloud facilitate communication and information exchange between participants.
7. Community clouds enable enterprises to increase or decrease their resources as needed in response to demand.(1)

Disadvantages of Community Cloud:

1. Security features are not as good as in a private cloud.
2. Unsuitable if there is no collaboration between participants.
3. Challenges arise in ensuring consistent performance and availability when multiple enterprises share the same resources.
4. The scalability options are limited as shared resources define the capacity of the community cloud.
5. The potential conflict of interests among community members regarding resource allocation and utilization.
6. Transparent governance frameworks and agreements are essential to address potential conflicts and ensure fair resource allocation.
7. Insufficient technical support and service level agreements compared to private or public cloud alternatives.

. 1. Tucakov, Dejan. What is Community Cloud? Benefits & Examples with Use Cases, JUNE 18, 2020. On site: https://cutt.us/ghrCz

Challenges of Cloud Computing

Despite the significance of cloud computing in collaboration and data storage, it encounters several challenges. Here is a summary of the most prominent among these challenges:

- **Security,** Since the advent of the internet, data security has consistently been a concern, and it is even more clear now that an increasing number of companies have transitioned to the cloud. Whether you are using it for personal or professional reasons, the cloud must remain secure by ensuring your cloud service provider has a good reputation in implementing stringent data security measures such as multi-factor authentication, data encryption, access control, and so forth.

Storing data in the cloud makes it more susceptible to hacking and cybercrimes. If you are not prepared, you are vulnerable to cyber risks such as phishing, ransomware attacks, identity theft, and malware infections, Which may lead to corruption of data stored on the cloud.

For instance, if the enterprise relies on it for data storage, it is crucial to ensure that only authorized individuals have access to it. Additionally, data encryption should be implemented, and it is essential to verify that the private cloud provider has sufficient security measures in place.

- **Performance challenge:** For instance, the performance of our cloud service platform may fail to meet our requirements. This could result in customer dissatisfaction with the enterprise's performance, leading to a reduction in its profits. Even a minor delay in cloud implementation can be a source of annoyance for the data owner. It is also essential to ensure that the cloud is not prone to outages.

Such incidents can cause disruptions in operations that depend on the data stored in it.

• The necessity of a contingency plan in the event of a power outage or natural disaster.

• The necessity of being cautious about the unintended buildup of your private cloud platform; for instance, if your cloud resources are not well-organized and optimized, storage space for files could accumulate quickly. This could result in paying for a larger storage package that you do not actually need[1].

1. The Reality of Using Cloud Computing Applications in Enabling Accounting Education: A Survey Study of the Opinions of Faculty Members in the Department of Financial and Accounting Sciences at 20 August 1955 University in Skikda, Algeria. Journal: Dafater Bouadex, Volume 11, Number: 02, 2022 AD.

Chapter Two

Digital Threats in Cloud Computing

- Data loss.
- Malware.
- Unauthorized access.

02

Data loss

Data loss is regarded as one of the most prevalent security risks in cloud computing, also known as data leakage. Data loss is the process in which information is deleted, destroyed, and rendered unreadable by a user, program, or application. In a cloud computing environment, data loss occurs when sensitive and crucial data is in the hands of someone else. The data owner cannot access one or more elements of the data, the hard drive malfunctions, or the software is not updated correctly.[1]

To tackle the challenge of data loss, encryption tools should be used whenever possible. And access controls to the cloud should be in place to restrict unauthorized users' access to sensitive information within the cloud environment. Business owners should also regularly review cloud service providers to ensure they adhere to best practices in cloud security. These steps assist in minimizing risks concerning data loss in cloud computing environments.

Overall, data loss can be attributed to several reasons. Below is an explanation of the most significant ones:

1. Accidental deletion (user error)

Unintended deletion is the most common source of data loss when using cloud storage. However, the automatic backup processes inherent in cloud computing solutions can recover deleted files or restore an older version of a document or database.

2. Overwriting data

It is also possible for information to be accidentally replaced by users or applications, and Software as a Service (SaaS) applications are a potential source of significant data loss, as these applications store large datasets and continuously update them. New information has the ability to overwrite old information, leading to data loss.

1. What are the Security Risks of Cloud Computing? Auditboard, on site: https://cutt.us/qJsln

3. Malware

Cloud storage service providers persist in their efforts to secure their networks and your data, thwarting all online attacks. Fortunately, thoroughly tested best practices and operational procedures are available to aid IT departments in securely managing access to data hosted in the cloud.

How to protect data stored in the cloud from loss.

1. Dedicate the required time and resources to formulate a backup and disaster recovery strategy, ensuring the backup of the most crucial data according to a timeline that aligns with business goals, ensuring timely retrieval when necessary.
2. Identifying a backup solution that aligns with the needs and priorities of the business is crucial, as not all solutions are created equal.
3. Ensure that there are multiple copies available for data recovery.
4. Consider how effectively your backup copies are stored in various data centers, ensuring that if there is an issue with one backup, information can be recovered from a different location.
5. Understanding the significance of storing data in a way that is tamper-resistant and impervious to encryption by ransomware(1).

1. Brandt, Charles. What Are the Chances of Losing Information in Cloud Storage? Marconet, August, 2023. On site: https://cutt.us/FFJGN

Malware

Here are various forms of malware attacks that are prevalent in cloud environments, as cyber attackers take advantage of the existence of crucial data on cloud platforms, aiming to infiltrate, pilfer the data, and subsequently extort the users.

Terms, cloud malware denotes harmful software created and distributed within cloud computing environments, aiming to pilfer data from users and enterprises, disrupt their operations, and induce diverse issues. Due to the interconnected nature of the cloud, the impact of a successful malware attack on the cloud can be catastrophic.

Here are the most damaging types of malware attacks in the cloud, typically affecting users working in any type of cloud environment:

1. Injection attacks

It is a cyber attack used by cybercriminals to create chaos in unprotected terminal servers through infiltration via unpatched access points. The goal is to steal data and identities, as well as distribute ransomware or exploit the stolen information. And the attacker can disable up to 100 systems at once with a single attack. And the best defense against this type of cloud malware attacks is to deploy specialized programs that can leverage the current strength of the cloud infrastructure to effectively control access and monitor the ongoing traffic using fast-acting cloud security tools.

2. Phishing Attacks

This type of attack involves sending emails or text messages that appear to be from known sources but are attempting to steal sensitive data or install malicious software instructions on the device.

To protect against phishing, it is essential to verify the authenticity of links before clicking on them, avoid opening attachments or unfamiliar messages, and use two-factor authentication.

3. Data theft

It is a common form of cloud malware attacks. For example, in 2013, 110 million users who made purchases at Target stores had their personal information stolen by internet criminals. The reason lies in the presence of an external vendor with weak systems, enabling attackers to access those cards, and it pertains to the company Fazio Mechanical Services, specialized in refrigeration services.

4. Trojan horses

It is a type of cloud malware that disguises itself as legitimate software to gain access to the system or steal data. Therefore, it is essential to avoid downloading any software from untrusted websites and refrain from opening suspicious email attachments.

5. Attacking serverless functions and application interfaces

Often, jobs and application programming interfaces are targeted without a server by advanced attackers who aim to access the enterprise's cloud environment.

This attack is executed by exploiting vulnerabilities in a serverless function or an application programming interface, allowing malicious actors to execute random or distorted code instructions on the system.

Therefore, enterprises should monitor their serverless functions and application programming interfaces for potential vulnerabilities, utilizing security scanning tools to detect any suspicious activity and ensuring that their serverless functions and application programming interfaces are always updated with the latest security patches.

6. Hypervisor DoS attacks

A Hypervisor program is a type of software that allows running multiple operating systems on the same computer simultaneously. Attacks occur when attackers attempt to overload the system by sending an excessive number of data or resource requests, leading to its disruption or unresponsiveness. To protect against this type of attack, it is crucial to ensure that your cloud security protocols are up-to-date and regularly monitored for any suspicious activity.

7. Exploiting live migration

Live migration is a process through which virtual machines can be moved from one physical host to another, allowing for improved resource utilization and enhanced performance. However, this process can be exploited by attackers in the presence of any security vulnerabilities in the system's security protocols.

8. Network eavesdropping

Eavesdropping on a Wi-Fi network is a method for remote access attacks, where attackers attempt to access a targeted device by intercepting and decrypting the network. Therefore, it is imperative to set a strong network password and ensure that devices are running the latest security patches.

9. zero-day exploit

It is a type of online attack that exploits previously unknown vulnerabilities in computer systems or applications. To prevent these attacks, it is essential to review the latest security patches and monitor any abnormal system behavior.[1]

1. The 10 Most Common Attack Types of Malware in the Cloud, What They Do and How to Defend Against Them, Buchanan. On site: https://cutt.us/PknJl

Unauthorized access

Unauthorized or illegal access is a significant threat to cloud security. A report highlighted cloud security, affirming that 53% of the surveyed enterprises consider unauthorized access through the misuse of employee credential data and insecure access controls as the single most prominent threat to cloud security. And 96% of the surveyed enterprises have some or all of their applications in the cloud. Access control can be addressed through cloud security solutions, alongside identity and access management policies.[1]

Identity and Access Management (IAM) is the security system that empowers suitable individuals to access the correct resources at the appropriate times and for valid reasons. Furthermore, secure application access enables the partitioning of access to cloud applications based on user trust. For instance, vendors require access to enterprise application relying solely on cloud access to the specific application needed to complete their tasks.

Hence, secure access to applications offers thorough tracking, monitoring, and reporting, facilitating information technology enterprises in adhering to data security regulations.

And there are key challenges to cloud security associated with unauthorized access:

1. Data breach

In 2021, there were reports of 738 data breaches, with hacking being the predominant cause. Therefore, ensuring the security of private information has become more crucial than ever. Additionally, there is a risk of data loss, either due to natural disasters such as fires or the theft of sensitive data.

2. Insecure entry points

When utilizing the cloud, you have the ability to access your data from any location and on any device. However, insecure interfaces, particularly application programming interfaces, present a threat that could be exploited for data theft and manipulation by identifying and exploiting programming flaws, commonly known as vulnerabilities[2].

1. Unauthorized access is the biggest threat to Cloud security, Cdnetworks, December 11, 2018. On site: https://cutt.us/r76hP
2. McCaw, Billy. 5 Key Cloud Security Challenges with unauthorized access, extreme compute, 2021. On site: https://cutt.us/OigBo

Chapter Three

How to Secure Cloud Computing from Digital Attacks

- Cloud security.
- Securing Data in cloud computing from hacking.

0 3

Cloud security

Cloud security involves procedures and technologies designed to secure cloud computing environments against both external and internal cybersecurity threats. Best practices in cloud security and carefully designed security management are essential to prevent unauthorized access, ensuring the security of data and applications in the cloud from current and emerging cybersecurity threats. Since data stored in the public cloud is managed by a third party and accessible over the internet, various challenges arise in maintaining a secure cloud.

In numerous instances, cloud services may be accessed beyond the enterprise network and from devices not overseen by the IT department. Within the external environment of a cloud service provider, IT teams experience reduced access to data compared to their control over servers and applications in their own workplaces. Cloud customers typically receive limited control by default, with no access to the physical infrastructure.

Users have the ability to access cloud applications and data over the internet, from any location or device, including the bring-your-own-device technology, thereby contributing to the security challenges. Furthermore, privileged access by employees of cloud service providers to user data has the potential to bypass their own security controls[1].

Generally, cloud computing offers users a centralised location for data and applications, alongside multiple endpoints and devices that necessitate security. Hence, security in cloud computing centrally oversees all your applications, devices, and data to guarantee comprehensive security. It streamlines task execution, facilitating the implementation of disaster recovery plans, optimizing network event monitoring, and refining web filtering, and strengthening DDoS security. DDoS attacks pose significant threats to cloud computing, targeting servers with large traffic simultaneously to inflict damage. Cloud security protects servers from these attacks through vigilant monitoring and distribution.

1. What is Cloud Security? sky high security. On site: https://cutt.us/3g7wy

The question here..... Is the cloud sufficiently secure for our sensitive content?

Users are increasingly dependent on cloud storage and processing, but they often worry that abandoning their security model might entail forfeiting their sole means of controlling access to their data. However, experience has demonstrated that this concern is baseless. Cloud service providers implement procedures and technologies to prevent their employees from accessing customer data. This prohibition usually involves encryption and company policies intended to prevent employees from viewing the data.

In practical terms, data breaches frequently result from a misconception regarding the users' role in securing their data or the misapplication of security tools offered as part of the cloud service. To clarify, cloud service providers are accountable for maintaining the operational environment for users, while users are accountable for events occurring within that environment.

Hence, in brief, the cloud can be secure for your content if you have a good understanding of cloud security tools.

In general, there are several issues that must be considered when selecting a cloud computing service provider, and the following provides an explanation of the most crucial ones:

1. Controls implemented to prevent data leakage

Look for service providers that have secure cloud computing controls designed to prevent problems like unauthorized access, data leakage, and data theft. This service should enable you to implement more precise security measures for your most critical data, including original security classifications. Therefore, the user should verify the accuracy of permission settings.

2. Strong authentication

Ensure that your cloud service provider provides strong authentication procedures to guarantee proper access through strong password controls and multi-factor authentication.

3. Data encryption

Ensure the ability to encrypt all data both at rest and during transfer and storage.

4. Vision and threat detection.

The provider of cloud computing services must utilize machine learning to recognize unwanted behavior, identify threats, and notify users. For instance, an analysis of data behavior might reveal that a member of the sales team in a particular enterprise tried to download confidential designs of products in a dubious manner.

5. Continuous commitment

Look for features that enable the management of the content lifecycle, including document retention and disposal, as well as electronic discovery.

6. Integrated security

Ensure the smooth integration of the provider's tools with your security suite through application programming interfaces. The tools provided by the provider are crucial for improving collaboration and smoothing internal and external workflows. Moreover, these tools should integrate seamlessly with all your applications, expanding security controls to any application the user might use to access their content without affecting their experience.[1].

Cloud service providers and their clients are jointly responsible for ensuring cloud security. The responsibility varies depending on the type of cloud services provided.

Here is an explanation of the differences in cloud security management based on the type of cloud:

- **Public cloud computing:** Managed by cloud service providers, servers are shared by multiple tenants in this environment.
- **Private cloud computing:** It might be located in a data centre owned or operated by the customer or a public cloud service provider. In both scenarios, it is regarded single-tenant servers, and enterprises do not need to share space with other companies.
- **Hybrid cloud computing:** It is combination of local data centres and external cloud services.
- **Community cloud:** It encompasses two or more cloud services managed by all cloud service providers.[Γ]

Regardless of the type of environment or set of environments users use, the primary goal of cloud security is to protect physical networks, including routers, electrical systems, data and data storage, data servers, applications, software, operating systems, and electronic devices.

1. What is cloud security? box. On site: https://cutt.us/j9fxI

2. . What is cloud security? box. On site: https://cutt.us/j9fxI

How does cloud security function?

• Infrastructure as a Service

In this model, cloud service providers provide computing, networking, and storage resources on demand. The provider is responsible for providing essential memory computing services. Customers are responsible for securing all aspects related to the operating system, encompassing applications, data, runtimes, middleware, and the operating system itself.

• Essential Service system

Cloud service providers provide a comprehensive development and usage environment in the cloud. They are responsible for securing runtime, middleware, the operating system, and essential memory computing services. Customers need to ensure the security of their applications, data, user access processes, as well as user devices and networks.

• Software as a Service

Customers can access the software through a pay-as-you-go service model, such as Microsoft Office 365 or Google Drive [1]

Irrespective of the party responsible for securing the data stored in the cloud, there are essential elements of cloud security. **The following provides an explanation of the most crucial ones:**

- **Restricting access,** as it is crucial to ensuring that only the right people are granted access to the right tools at the right time.
- **Securing Data,** because users of cloud computing services need to know the location of their data and establish appropriate controls to secure the data and infrastructure hosting that data.
- **Data recovery,** there must be good backups of the data and a data recovery plan to avoid any damage in the event of a security breach.
- **Response plan,** when exposed to attacks, there must be a plan to mitigate the impact of these attacks.
- **Checking for security** vulnerabilities at an early stage.
- **Directing the focus of security teams towards eliminating emerging threats** by enhancing cloud resource configurations through software to reduce security issues faced by production environments.

1. . What is cloud security? box. On site: https://cutt.us/j9fxl

Securing Data in cloud against hacking

Hacking is one of the main threats to data stored in the cloud. To secure it from this threat, it is essential to ensure the adoption of the following measures

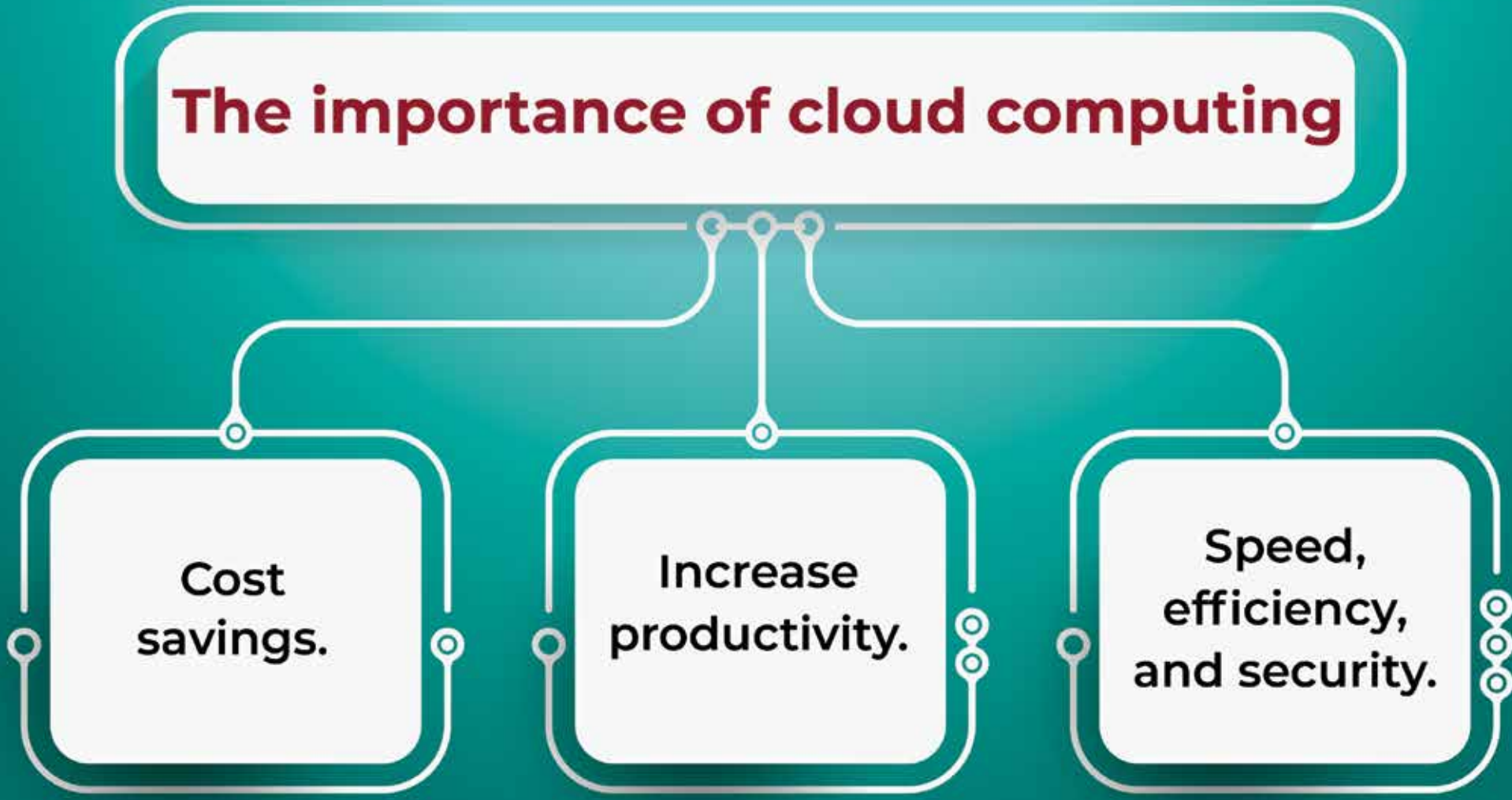
- To optimize the advantages of cloud computing, it is essential to utilize strong passwords that include letters, numbers, and special characters.
- Secure all the devices you use to access your cloud data, including smartphones and tablets, especially if your data is synchronized across multiple devices.
- Create regular backups of your data so that you can fully recover it in case of a cloud service outage or data loss from the cloud service provider, whether by storing a copy on your home computer, an external hard drive, or even transferring it from one cloud service to another, as long as the cloud service providers do not share the same infrastructure.
- Use permissions to prevent any individual or device from accessing all your data. If you have a home network, use guest networks for your children, internet of things devices, and the television, and reserve the «access all areas» permission for your personal use.
- Use antivirus and anti-malware software.
- Avoid accessing your data on public Wi-Fi networks, especially if you are not using strong authentication.
- Multi-Factor Authentication (MFA) is an intelligent way to secure your access, whether through fingerprints, a password, or a separate code sent to your mobile device.
- If you no longer use a service or program, close it properly, and make sure not to leave an old account open, as hackers exploit such accounts to find a loophole into your system and devices.[1]

1. . What is cloud computing? Kaspersky. available on the link: https://cutt.us/CO2Zq


Training cards

Cloud computing

Refers to accessing a range of services, including tools and applications, such as data storage, servers, databases, networks, and software, over the internet. Instead of storing files on your local hard drive or private drive, you can store documents in a database on the network using the cloud.


The importance of cloud computing
Cost savings.
Increase productivity.
Speed, efficiency, and security.

Public cloud computing

It is available to everyone to store and access information online using the pay-as-you-go model. The compute resources are managed and operated by a cloud service provider who takes care of the supporting infrastructure and ensures that resources are available and scalable for users.

Private cloud computing

It is also known as an internal cloud or corporate cloud, and is employed by enterprises to create and manage their private data centres, either in-house or through external service providers.

Hybrid cloud:

It is a combination of public and private cloud computing. In this type of clouds, enterprises can leverage the advantages of both public and private clouds to create a flexible and scalable computing environment.

Community Cloud:

It permits access to systems and services provided by consortium of multiple enterprises for the purpose of sharing information within the enterprise and a particular community.

It is owned and managed by one or more enterprises within the community, a third party, or a consortium of them. Such as: The healthcare community cloud.

Data loss

It is regarded as one of the most prevalent security risks in cloud computing, also known as 'data leakage.' Data loss is the process in which information is deleted, destroyed, and rendered unreadable by a user, program, or application.

Cloud malware

Cloud malware denotes harmful software created and distributed within cloud computing environments, aiming to pilfer data from users and enterprises, disrupt their operations, and induce diverse issues.

Hypervisor DoS attacks

A Hypervisor program is a type of software that allows running multiple operating systems on the same computer simultaneously.

Attacks occur when attackers attempt to overload the system by sending an excessive number of data or resource requests, leading to its disruption or unresponsiveness.

Trojan horses

It is a type of cloud malware that disguises itself as legitimate software to gain access to the system or steal data.

Phishing attacks

It involves sending emails or text messages that appear to be from known sources but are attempting to steal sensitive data or install malicious software instructions on the device.

Injection attacks

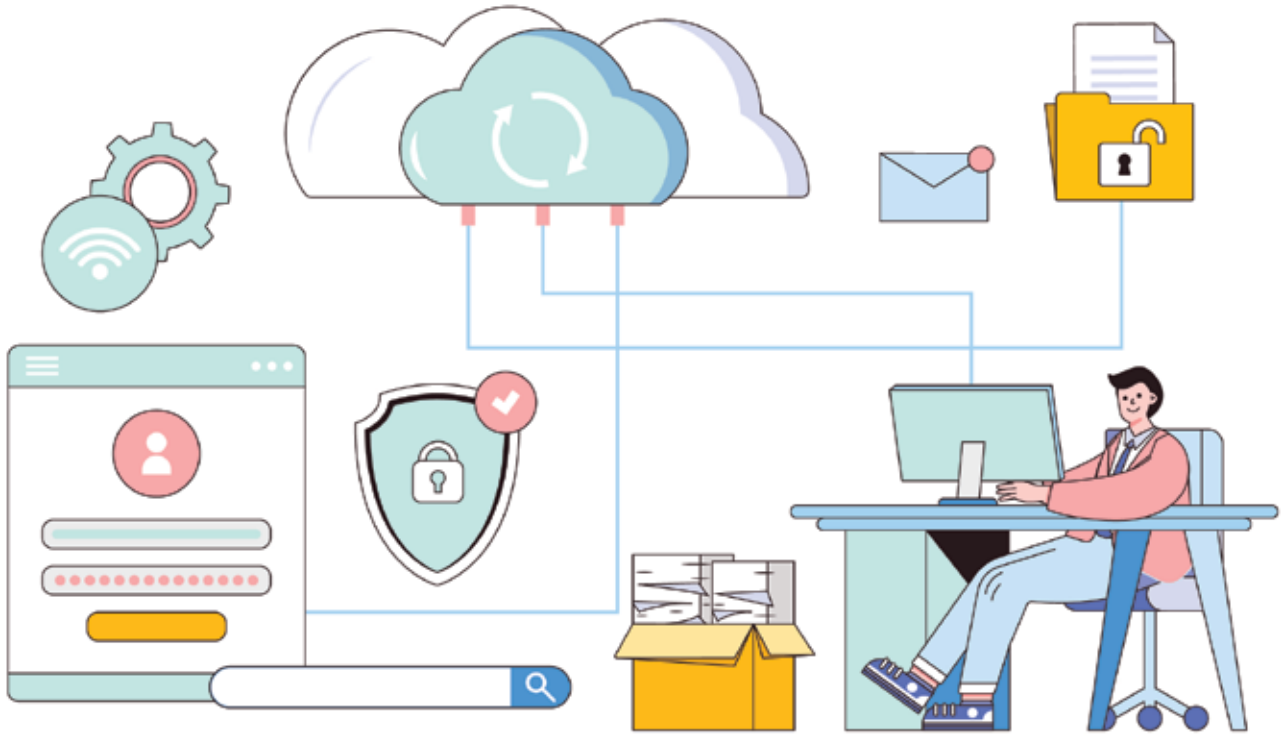
It is a cyber attackused by cybercriminals to create chaos in unprotected terminal servers through infiltration via unpatched access points. The goal is to steal data and identities, as well as distribute ransomware or exploit the stolen information.

Live migration

It is a process through which virtual machines can be moved from one physical host to another, allowing for improved resource utilization and enhanced performance. However, this process can be exploited by attackers in the presence of any security vulnerabilities in the system's security protocols.

Zero-day exploit

It is called "Zero-Day Attack" a type of online attack that exploits previously unknown vulnerabilities in computer systems or applications.



Cloud security

It involves procedures and technologies designed to secure cloud computing environments against both external and internal cybersecurity threats.

Security in cloud computing centrally oversees all your applications, devices, and data to guarantee comprehensive security. It streamlines task execution, facilitating the implementation of disaster recovery plans, optimizing network event monitoring, refining web filtering.

DDoS attacks

DDoS attacks pose significant threats to cloud computing, targeting servers with large traffic simultaneously to inflict damage. Cloud security protects servers from these attacks by monitoring and addressing them immediately upon occurrence.


Sketches

How to prevent data loss in the cloud?

1. Create backups of the most critical data.
2. Store your backups in various data centres.
3. Understanding the significance of storing data in a way that is tamper-resistant and impervious to encryption by ransomware.

What are the reasons for data loss in the cloud?

1. Accidental deletion (user error).
2. Overwriting data.
3. Harmful actions.

What is the reason behind the naming of cloud computing?

The reason for this name is that the accessed information is stored remotely in the cloud or virtual space. Companies that offer cloud services enable users to store files and applications on remote servers, allowing access to all data over the internet.

References

Arabic references:

1. What is cloud security?, Microsoft. Available at: cutt.us/tS1Fl
2. What is cloud security? Kaspersky, available at: https://cutt.us/CO2Zq
3. The reality of using cloud computing applications in activating accounting education, an exploratory study of the opinions of professors of the Department of Financial Sciences and Accounting at the University of Algiers, Budex Notebooks Magazine, Volume 11

English references:

1. 6 Advantages and Disadvantages of Private Cloud | Limitations & Benefits of Private Cloud, hitechwhizz. On site: https://cutt.us/CplCr
2. Brandt, Charles. What Are the Chances of Losing Information in Cloud Storage? Marconet, August, 2023. On site: https://cutt.us/FFJGN
3. Frankenfield, Jake. What is Cloud Computing? Pros and Cons of Different Types of Services, investopedia, April 2023. On site: https://www.investopedia.com/terms/c/cloud-computing.asp
4. Linao, Portia. Why is it called "The Cloud"? officesolutionsit, February 2023. On site: https://www.officesolutionsit.com.au/blog/why-is-it-called-the-cloud
5. McCaw, Billy. 5 Key Cloud Security Challenges with unauthorized access, extreme compute, 2021. On site: https://cutt.us/OigBo
6. Mohanakrishnan, Ramya. What Is Community Cloud? Definition, Architecture, Examples, and Best Practices, spiceworks. On site: https://cutt.us/ORUiy
7. Public and Private Cloud Advantages and Disadvantages, connectria. On site: https://cutt.us/cMN8I
8. Stephen J. Bigelow. What is public cloud? Everything you need to know, techtarget. On site: https://www.techtarget.com/searchcloudcomputing/definition/public-cloud

9. The 10 Most Common Attack Types of Malware in the Cloud, What They Do and How to Defend Against Them, Buchanan. On site: https://cutt.us/PknJI

10. Tucakov, Dejan. What is Community Cloud? Benefits & Examples with Use Cases, JUNE 18, 2020. On site: https://cutt.us/ghrCz

11. Types of Cloud, javatpoint. On site: https://www.javatpoint.com/types-of-cloud

12. Unauthorized access is the biggest threat to Cloud security, Cdnetworks, December 11, 2018. On site: https://cutt.us/r76hP

13. Weinberger, Matt. Why 'cloud computing' is called 'cloud computing', businessinsider, Mar 2015. On site: https://www.businessinsider.in/why-cloud-computing-is-called-cloud-computing/articleshow/46544750.cms

14. What are the Security Risks of Cloud Computing? Auditboard, on site: https://cutt.us/qJsln

15. What is Cloud Security? sky high security. On site: https://cutt.us/3g7wy

16. What is cloud security? box. On site: https://cutt.us/j9fxI

17. What is cloud security? box. On site: https://cutt.us/j9fxI

18. What is hybrid cloud? netapp. On site: https://cutt.us/8N9QZ

19. What is private cloud? ovhcloud. On site: https://www.ovhcloud.com/en-gb/learn/what-is-private-cloud/

20. What is private cloud? Types, process, benefits, examples, knowledgehut. On site: https://2u.pw/vtxJ57Q


CyberEco


الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

CyberEco

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency