Cloud computing security

[Jump to navigation](https://en.wikipedia.org/wiki/Cloud_computing_security#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Cloud_computing_security#searchInput)

*For cloud-hosted security software, see*[*Security as a service*](https://en.wikipedia.org/wiki/Security_as_a_service)*.*

## **Cloud computing security** or, more simply, **cloud security** refers to a broad set of policies, technologies, applications, and controls utilized to protect virtualized IP, data, applications, services, and the associated infrastructure of [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing). It is a sub-domain of [computer security](https://en.wikipedia.org/wiki/Computer_security), [network security](https://en.wikipedia.org/wiki/Network_security), and, more broadly, [information security](https://en.wikipedia.org/wiki/Information_security). **Security issues associated with the cloud[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=1" \o "Edit section: Security issues associated with the cloud)]**

Cloud [computing](https://en.wikipedia.org/wiki/Computing) and storage provide users with capabilities to store and process their data in third-party [data centers](https://en.wikipedia.org/wiki/Data_center).[[1]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-cloudid-1) Organizations use the cloud in a variety of different service models (with acronyms such as [SaaS](https://en.wikipedia.org/wiki/SaaS), [PaaS](https://en.wikipedia.org/wiki/PaaS" \o "PaaS), and [IaaS](https://en.wikipedia.org/wiki/IaaS" \o "IaaS)) and deployment models ([private](https://en.wikipedia.org/wiki/Cloud_computing#Private_cloud), [public](https://en.wikipedia.org/wiki/Cloud_computing#Public_cloud), [hybrid](https://en.wikipedia.org/wiki/Cloud_computing#Hybrid_cloud), and [community](https://en.wikipedia.org/wiki/Community_cloud)).[[2]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Srinivasan-2)

Security concerns associated with cloud computing are typically categorized in two ways: as security issues faced by cloud providers (organizations providing [software-](https://en.wikipedia.org/wiki/Software_as_a_service), [platform-](https://en.wikipedia.org/wiki/Platform_as_a_service), or [infrastructure-as-a-service](https://en.wikipedia.org/wiki/Infrastructure_as_a_service) via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud).[[3]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-3) The responsibility is shared, however, and is often detailed in a cloud provider's "shared security responsibility model" or "shared responsibility model."[[4]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-CSACloudCont4-4)[[5]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-AWSShared20-5)[[6]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-TozziAvoid20-6) The provider must ensure that their infrastructure is secure and that their clients’ data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.[[5]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-AWSShared20-5)[[6]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-TozziAvoid20-6)

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a 2010 [Cloud Security Alliance](https://en.wikipedia.org/wiki/Cloud_Security_Alliance) report, insider attacks are one of the top seven biggest threats in cloud computing.[[7]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Top_Threats_to_Cloud_Computing_v1.0-7) Therefore, cloud service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers are recommended to be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, cloud service providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper [data isolation](https://en.wikipedia.org/wiki/Isolation_(database_systems)) and logical storage segregation.[[2]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Srinivasan-2)

The extensive use of [virtualization](https://en.wikipedia.org/wiki/Virtualization) in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service.[[8]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Cloud_Virtual_Security_Winkler-8) Virtualization alters the relationship between the OS and underlying hardware – be it computing, storage or even networking. This introduces an additional layer – virtualization – that itself must be properly configured, managed and secured.[[9]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-virtualization_risks_hickey-9) Specific concerns include the potential to compromise the virtualization software, or "[hypervisor](https://en.wikipedia.org/wiki/Hypervisor)". While these concerns are largely theoretical, they do exist.[[10]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Securing_the_Cloud_Winkler_virt-10) For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole data center to go down or be reconfigured to an attacker's liking.

## **Cloud security controls[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=2" \o "Edit section: Cloud security controls)]**

Cloud security architecture is effective only if the correct defensive implementations are in place. An efficient cloud security architecture should recognize the issues that will arise with security management and follow all of the best practices, procedures, and guidelines to ensure a secure cloud environment. Security management addresses these issues with security controls. These controls protect cloud environments and are put in place to safeguard any weaknesses in the system and reduce the effect of an attack. While there are many types of controls behind a cloud security architecture, they can usually be found in one of the following categories:

**Deterrent controls**

These controls are administrative mechanisms intended to reduce attacks on a cloud system and are utilized to ensure compliance with external controls. Much like a warning sign on a fence or a property, deterrent controls typically reduce the threat level by informing potential attackers that there will be adverse consequences for them if they proceed.[[11]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-11) (Some consider them a subset of preventive controls.) Examples of such controls could be considered as policies, procedures, standards, guidelines, laws, and regulations that guide an organization towards security. Although most malicious actors ignore such deterrent controls, such controls are intended to ward off those who are inexperienced or curious about compromising the IT infrastructure of an organization.

**Preventive controls**

The main objective of preventive controls is to strengthen the system against incidents, generally by reducing if not actually eliminating vulnerabilities, as well as preventing unauthorized intruders from accessing or entering the system.[[12]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-12) This could be achieved by either *adding* software or feature implementations (such as firewall protection, endpoint protection, and multi-factor authentication), or *removing* unneeded functionalities so that the attack surface is minimized (as in [unikernel](https://en.wikipedia.org/wiki/Unikernel" \o "Unikernel) applications). Additionally, educating individuals through security awareness training and exercises is included in such controls due to the human error being the weakest point of security. Strong authentication of cloud users, for instance, makes it less likely that unauthorized users can access cloud systems, and more likely that cloud users are positively identified. All in all, preventative controls affect the likelihood of a loss event occurring and are intended to prevent or eliminate the systems’ exposure to malicious action.

**Detective controls**

Detective controls are intended to detect and react appropriately to any incidents that occur. In the event of an attack, a detective control will signal the preventative or corrective controls to address the issue. Detective security controls function not only when such an activity is in progress and after it has occurred. System and network security monitoring, including intrusion detection and prevention arrangements, are typically employed to detect attacks on cloud systems and the supporting communications infrastructure. Most organizations acquire or create a dedicated security operations center (SOC), where dedicated members continuously monitor the organization’s IT infrastructure through logs and Security Information and Event Management (SIEM) software. SIEMs are security solutions that help organizations and security teams analyze “log data in real-time for swift detection of security incidents.”[[13]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-13) SIEMS are not the only examples of detective controls. There are also Physical security controls, Intrusion detection systems, and anti-virus/anti-malware tools, which all have different functions centered around the exact purpose of detecting security compromises within an IT infrastructure.

**Corrective controls**

Corrective controls reduce the consequences of an incident, generally by limiting the damage. Such controls include technical, physical, and administrative measures that occur during or after an incident to restore the systems or resources to their previous state after a security incident.[[14]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-14) There are plenty of examples of corrective controls, both physical and technical. For instance, re-issuing an access card or repairing physical damage can be considered corrective controls. However, technical controls such as terminating a process and administrative controls such as implementing an incident response plan could also be considered corrective controls. Corrective controls are focused on recovering and repairing any damage caused by a security incident or unauthorized activity. The value is needed to change the function of security.

## **Dimensions of cloud security[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=3" \o "Edit section: Dimensions of cloud security)]**

Cloud security engineering is characterized by the security layers, plan, design, programming, and best practices that exist inside a cloud security arrangement. Cloud security engineering requires the composed and visual model (design and UI) to be characterized by the tasks inside the Cloud. This cloud security engineering process includes such things as access to the executives, techniques, and controls to ensure applications and information. It also includes ways to deal with and keep up with permeability, consistency, danger stance, and by and large security. Processes for imparting security standards into cloud administrations and activities assume an approach that fulfills consistent guidelines and essential framework security parts.[[15]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-15)

For interest in Cloud advancements to be viable, companies should recognize the various parts of the Cloud and how they remain to impact and help them. These interests may include investments in cloud computing and security, for example. This of course leads to leads to driving push for the Cloud advancements to succeed.

Though the idea of [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) isn't new, associations are increasingly enforcing it because of its flexible scalability, relative trustability, and cost frugality of services. However, despite its rapid-fire relinquishment in some sectors and disciplines, it's apparent from exploration and statistics that security-related pitfalls are the most conspicuous hedge to its wide relinquishment.[*[citation needed](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "Wikipedia:Citation needed)*]

It is generally recommended that information security controls be selected and implemented according to and in proportion to the risks, typically by assessing the threats, vulnerabilities and impacts. Cloud security concerns can be grouped in various ways; Gartner named seven[[16]](https://en.wikipedia.org/wiki/Cloud_computing_security" \l "cite_note-16) while the [Cloud Security Alliance](https://en.wikipedia.org/wiki/Cloud_Security_Alliance) identified twelve areas of concern.[[17]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-17) [Cloud access security brokers](https://en.wikipedia.org/wiki/Cloud_access_security_broker) (CASBs) are software that sits between cloud users and cloud applications to provide visibility into cloud application usage, data protection and governance to monitor all activity and enforce security policies.[[18]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-18)

## **Security and privacy**

Any service without a "hardened" environment is considered a "soft" target. Virtual servers should be protected just like a physical server against [data leakage](https://en.wikipedia.org/wiki/Data_leakage_prevention), [malware](https://en.wikipedia.org/wiki/Malware), and exploited vulnerabilities. "Data loss or leakage represents 24.6% and cloud related malware 3.4% of threats causing cloud outages”[[19]](https://en.wikipedia.org/wiki/Cloud_computing_security" \l "cite_note-19)

### Identity management**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=5" \o "Edit section: Identity management)]**

Every enterprise will have its own [identity management system](https://en.wikipedia.org/wiki/Identity_management_system) to control access to information and computing resources. Cloud providers either integrate the customer's identity management system into their own infrastructure, using [federation](https://en.wikipedia.org/wiki/Federated_identity_management) or [SSO](https://en.wikipedia.org/wiki/Single_sign-on) technology or a biometric-based identification system,[[1]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-cloudid-1) or provide an identity management system of their own.[[20]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-20) CloudID,[[1]](https://en.wikipedia.org/wiki/Cloud_computing_security" \l "cite_note-cloudid-1) for instance, provides privacy-preserving cloud-based and cross-enterprise biometric identification. It links the confidential information of the users to their biometrics and stores it in an encrypted fashion. Making use of a searchable encryption technique, biometric identification is performed in the encrypted domain to make sure that the cloud provider or potential attackers do not gain access to any sensitive data or even the contents of the individual queries.[[1]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-cloudid-1)

### Physical security**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=6" \o "Edit section: Physical security)]**

Cloud service providers physically secure the IT [hardware](https://en.wikipedia.org/wiki/Computer_hardware) (servers, routers, cables etc.) against unauthorized access, interference, theft, fires, floods etc. and ensure that essential supplies (such as electricity) are sufficiently robust to minimize the possibility of disruption. This is normally achieved by serving cloud applications from professionally specified, designed, constructed, managed, monitored and maintained data centers.

### Personnel security**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=7" \o "Edit section: Personnel security)]**

Various information security concerns relating to the IT and other professionals associated with cloud services are typically handled through pre-, para- and post-employment activities such as security screening potential recruits, security awareness and training programs, and proactive.

### Privacy**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=8" \o "Edit section: Privacy)]**

Providers ensure that all critical data (credit card numbers, for example) are [masked](https://en.wikipedia.org/wiki/Data_masking) or encrypted and that only authorized users have access to data in its entirety. Moreover, digital identities and credentials must be protected as should any data that the provider collects or produces about customer activity in the cloud.

### Penetration testing**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=9" \o "Edit section: Penetration testing)]**

[Penetration testing](https://en.wikipedia.org/wiki/Penetration_test) is the process of performing offensive security tests on a system, service, or [computer network](https://en.wikipedia.org/wiki/Computer_network) to find security weaknesses in it. Since the cloud is a shared environment with other customers or tenants, following penetration testing rules of engagement step-by-step is a mandatory requirement. Scanning and penetration testing from inside or outside the cloud should be authorized by the cloud provider. Violation of acceptable use policies can lead to termination of the service.[[21]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-21)

### Cloud vulnerability and penetration testing**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=10" \o "Edit section: Cloud vulnerability and penetration testing)]**

Scanning the cloud from outside and inside using free or commercial products is crucial because without a hardened environment your service is considered a soft target. Virtual servers should be hardened just like a physical server against [data leakage](https://en.wikipedia.org/wiki/Data_leakage_prevention), malware, and exploited vulnerabilities. "Data loss or leakage represents 24.6% and cloud-related malware 3.4% of threats causing cloud outages”

Scanning and penetration testing from inside or outside the cloud must be authorized by the cloud provider. Since the cloud is a shared environment with other customers or tenants, following penetration testing rules of engagement step-by-step is a mandatory requirement. Violation of acceptable use policies can lead to the termination of the service. Some key terminology to grasp when discussing penetration testing is the difference between application and network layer testing. Understanding what is asked of you as the tester is sometimes the most important step in the process. The network-layer testing refers to testing that includes internal/external connections as well as the interconnected systems throughout the local network. Oftentimes, social engineering attacks are carried out, as the most vulnerable link in security is often the employee.

**White-box testing**

Testing under the condition that the “attacker” has full knowledge of the internal network, its design, and implementation.

**Grey-box testing**

Testing under the condition that the “attacker” has partial knowledge of the internal network, its design, and implementation.

**Black-box testing**

Testing under the condition that the “attacker” has no prior knowledge of the internal network, its design, and implementation.

## **Data security[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=11" \o "Edit section: Data security)]**

There are numerous security threats associated with cloud data services. This includes traditional threats and non-traditional threats. Traditional threats include: [network eavesdropping](https://en.wikipedia.org/wiki/Network_eavesdropping), illegal invasion, and denial of service attacks, but also specific cloud computing threats, such as side channel attacks, virtualization vulnerabilities, and abuse of cloud services. In order to mitigate these threats security controls often rely on monitoring the three areas of the CIA triad. The CIA Triad refers to confidentiality, integrity, as well as access controllability which can be further understood from the following.[[22]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-22)

It is important to note that many effective security measures cover several or all of the three categories. Encryption for example prevents unauthorized access and as a result ensures the confidentiality, availability, and integrity of the data. Backups on the other hand generally cover integrity and firewalls only cover confidentiality and access controllability.[[23]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-23)

### Confidentiality**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=12" \o "Edit section: Confidentiality)]**

Data confidentiality is the property in that data contents are not made available or disclosed to illegal users. Outsourced data is stored in a cloud and out of the owners' direct control. Only authorized users can access the sensitive data while others, including CSPs, should not gain any information about the data. Meanwhile, data owners expect to fully utilize cloud data services, e.g., data search, data computation, and [data sharing](https://en.wikipedia.org/wiki/Data_sharing), without the leakage of the data contents to CSPs or other adversaries. Confidentiality refers to how data must be kept strictly confidential to the owner of said data

An example of security control that covers confidentiality is encryption so that only authorized users can access the data.

### Access controllability**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=13" \o "Edit section: Access controllability)]**

Access controllability means that a data owner can perform the selective restriction of access to their data outsourced to the cloud. Legal users can be authorized by the owner to access the data, while others can not access it without permission. Further, it is desirable to enforce fine-grained [access control](https://en.wikipedia.org/wiki/Computer_access_control) to the outsourced data, i.e., different users should be granted different access privileges with regard to different data pieces. The access authorization must be controlled only by the owner in untrusted cloud environments.

Access control can also be referred to as availability. While unauthorized access should be strictly prohibited, access for administrative or even consumer uses should be allowed but monitored as well. Availability and Access control ensure that the proper amount of permissions is granted to the correct persons.

### Integrity**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=14" \o "Edit section: Integrity)]**

[Data integrity](https://en.wikipedia.org/wiki/Data_integrity) demands maintaining and assuring the accuracy and completeness of data. A data owner always expects that her or his data in a cloud can be stored correctly and trustworthy. It means that the data should not be illegally tampered with, improperly modified, deliberately deleted, or maliciously fabricated. If any undesirable operations corrupt or delete the data, the owner should be able to detect the corruption or loss. Further, when a portion of the outsourced data is corrupted or lost, it can still be retrieved by the data users. Effective integrity security controls go beyond protection from malicious actors and protect data from unintentional alterations as well.

## **Risks and vulnerabilities of Cloud Computing[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=15" \o "Edit section: Risks and vulnerabilities of Cloud Computing)]**

While cloud computing is on the cutting edge of information technology there are risks and vulnerabilities to consider before investing fully in it. Security controls and services do exist for the cloud but as with any security system they are not guaranteed to succeed. Furthermore, some risks extend beyond asset security and may involve issues in productivity and even privacy as well.[[24]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-24)

### Privacy Concerns**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=16" \o "Edit section: Privacy Concerns)]**

Cloud computing is still an emerging technology and thus is developing in relatively new technological structures. As a result, all cloud services must undertake Privacy Impact Assessments or PIAs before releasing their platform. Consumers as well that intend to use clouds to store their customer's data must also be aware of the vulnerabilities of having non-physical storage for private information.[[25]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Svantesson_&_Clarke_2010-25)

### Unauthorized Access to Management interface**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=17" \o "Edit section: Unauthorized Access to Management interface)]**

Due to the autonomous nature of the cloud, consumers are often given management interfaces to monitor their databases. By having controls in such a congregated location and by having the interface be easily accessible for convenience for users, there is a possibility that a single actor could gain access to the cloud's management interface; giving them a great deal of control and power over the database.[[26]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Grobauer_Walloschek_&_Stocker_2011-26)

### Data Recovery Vulnerabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=18" \o "Edit section: Data Recovery Vulnerabilities)]**

The cloud's capabilities with allocating resources as needed often result in resources in memory and otherwise being recycled to another user at a later event. For these memory or storage resources, it could be possible for current users to access information left by previous ones.[[26]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Grobauer_Walloschek_&_Stocker_2011-26)

### Internet Vulnerabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=19" \o "Edit section: Internet Vulnerabilities)]**

The cloud requires an internet connection and therefore internet protocols to access. Therefore, it is open to many internet protocol vulnerabilities such as man-in-the-middle attacks. Furthermore, by having a heavy reliance on internet connectivity, if the connection fails consumers will be completely cut off from any cloud resources.[[26]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Grobauer_Walloschek_&_Stocker_2011-26)

### Encryption Vulnerabilities**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=20" \o "Edit section: Encryption Vulnerabilities)]**

Cryptography is an ever-growing field and technology. What was secure 10 years ago may be considered a significant security risk by today's standards. As technology continues to advance and older technologies grow old, new methods of breaking encryptions will emerge as well as fatal flaws in older encryption methods. Cloud providers must keep up to date with their encryption as the data they typically contain is especially valuable.[[27]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-27)

### Legal issues**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=21" \o "Edit section: Legal issues)]**

Privacy legislation often varies from country to country. By having information stored via the cloud it is difficult to determine under which jurisdictions the data falls under. Transborder clouds are especially popular given that the largest companies transcend several countries. Other legal dilemmas from the ambiguity of the cloud refer to how there is a difference in privacy regulation between information shared between and information shared inside of organizations.[[25]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Svantesson_&_Clarke_2010-25)

### Attacks**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=22" \o "Edit section: Attacks)]**

There are several different types of attacks on cloud computing, one that is still very much untapped is infrastructure compromise. Though not completely known it is listed as the attack with the highest amount of payoff.[[28]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-28) What makes this so dangerous is that the person carrying out the attack is able to gain a level of privilege of having essentially root access to the machine. It is very hard to defend against attacks like these because they are so unpredictable and unknown, attacks of this type are also called [zero day exploits](https://en.wikipedia.org/wiki/Zero_day_exploits) because they are difficult to defend against since the vulnerabilities were previously unknown and unchecked until the attack has already occurred.

[DoS](https://en.wikipedia.org/wiki/Denial-of-service_attack) attacks aim to have systems be unavailable to their users. Since cloud computing software is used by large numbers of people, resolving these attacks is increasingly difficult. Now with cloud computing on the rise, this has left new opportunities for attacks because of the virtualization of data centers and cloud services being utilized more.[[29]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-29)

With the global pandemic that started early in 2020 taking effect, there was a massive shift to remote work, because of this companies became more reliant on the cloud. This massive shift has not gone unnoticed, especially by cybercriminals and bad actors, many of which saw the opportunity to attack the cloud because of this new remote work environment. Companies have to constantly remind their employees to keep constant vigilance especially remotely. Constantly keeping up to date with the latest security measures and policies, mishaps in communication are some of the things that these cybercriminals are looking for and will prey upon.

Moving work to the household was critical for workers to be able to continue, but as the move to remote work happened, several security issues arose quickly. The need for data privacy, using applications, personal devices, and the internet all came to the forefront. The pandemic has had large amounts of data being generated especially in the healthcare sector. Big data is accrued for the healthcare sector now more than ever due to the growing coronavirus pandemic. The cloud has to be able to organize and share the data with its users securely. Quality of data looks for four things: accuracy, redundancy, completeness and consistency.[[30]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-30)

Users had to think about the fact that massive amounts of data are being shared globally. Different countries have certain laws and regulations that have to be adhered to. Differences in policy and jurisdiction give rise to the risk involved with the cloud. Workers are using their personal devices more now that they are working from home. Criminals see this increase as an opportunity to exploit people, software is developed to infect people's devices and gain access to their cloud. The current pandemic has put people in a situation where they are incredibly vulnerable and susceptible to attacks. The change to remote work was so sudden that many companies simply were unprepared to deal with the tasks and subsequent workload they have found themselves deeply entrenched in. Tighter security measures have to be put in place to ease that newfound tension within organizations.

## **Encryption[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=23" \o "Edit section: Encryption)]**

Some advanced [encryption](https://en.wikipedia.org/wiki/Encryption) algorithms which have been applied to cloud computing increase the protection of privacy. In a practice called [crypto-shredding](https://en.wikipedia.org/wiki/Crypto-shredding), the keys can simply be deleted when there is no more use of the data



.

### Attribute-based encryption (ABE)**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=24" \o "Edit section: Attribute-based encryption (ABE))]**

[Attribute-based encryption](https://en.wikipedia.org/wiki/Attribute-based_encryption) is a type of [public-key encryption](https://en.wikipedia.org/wiki/Public-key_encryption) in which the [secret key](https://en.wikipedia.org/wiki/Secret_key) of a user and the ciphertext are dependent upon attributes (e.g. the country in which he lives, or the kind of subscription he has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext.

Some of the strengths of Attribute-based encryption are that it attempts to solve issues that exist in current public-key infrastructure(PKI) and identity-based encryption(IBE) implementations. By relying on attributes ABE circumvents needing to share keys directly, as with PKI, as well as having to know the identity of the receiver, as with IBE.

These benefits come at a cost as ABE suffers from the decryption key re-distribution problem. Since decryption keys in ABE only contain information regarding access structure or the attributes of the user it is hard to verify the user's actual identity. Thus malicious users can intentionally leak their attribute information so that unauthorized users can imitate and gain access.[[31]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-31)

#### Ciphertext-policy ABE (CP-ABE)**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=25" \o "Edit section: Ciphertext-policy ABE (CP-ABE))]**

Ciphertext-policy ABE (CP-ABE) is a type of public-key encryption. In the CP-ABE, the encryptor controls the access strategy. The main research work of CP-ABE is focused on the design of the access structure. A Ciphertext-policy attribute-based encryption scheme consists of four algorithms: Setup, Encrypt, KeyGen, and Decrypt.[[32]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-32) The Setup algorithm takes security parameters and an attribute universe description as input and outputs public parameters and a master key. The encryption algorithm takes data as input. It then encrypts it to produce ciphertext that only a user that possesses a set of attributes that satisfies the access structure will decrypt the message. The KeyGen algorithm then takes the master key and the user's attributes to develop a private key. Finally, the Decrypt algorithm takes the public parameters, the ciphertext, the private key, and user attributes as input. With this information, the algorithm first checks if the users’ attributes satisfy the access structure and then decrypts the ciphertext to return the data.

#### Key-policy ABE (KP-ABE)**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=26" \o "Edit section: Key-policy ABE (KP-ABE))]**

Key-policy Attribute-Based Encryption, or KP-ABE, is an important type of [Attribute-Based Encryption](https://en.wikipedia.org/wiki/Attribute-based_encryption). KP-ABE allows senders to encrypt their messages under a set of attributes, much like any Attribute Based Encryption system. For each encryption, private user keys are then generated which contain decryption algorithms for deciphering the message and these private user keys grant users access to specific messages that they correspond to. In a KP-ABE system, [ciphertexts](https://en.wikipedia.org/wiki/Ciphertext" \o "Ciphertext), or the encrypted messages, are tagged by the creators with a set of attributes, while the user's private keys are issued that specify which type of ciphertexts the key can decrypt.[[33]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-33) The private keys control which ciphertexts a user is able to decrypt.[[34]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-34) In KP-ABE, the attribute sets are used to describe the encrypted texts and the private keys are associated to the specified policy that users will have for the decryption of the ciphertexts. A drawback to KP-ABE is that in KP-ABE the encryptor does not control who has access to the encrypted data, except through descriptive attributes, which creates a reliance on the key-issuer granting and denying access to users. Hence, the creation of other ABE systems such as Ciphertext-Policy Attribute-Based Encryption.[[35]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-35)

### Fully homomorphic encryption (FHE)**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=27" \o "Edit section: Fully homomorphic encryption (FHE))]**

[Fully Homomorphic Encryption](https://en.wikipedia.org/wiki/Fully_homomorphic_encryption) is a cryptosystem that supports arbitrary computation on ciphertext and also allows computing sum and product for the encrypted data without decryption. Another interesting feature of Fully Homomorphic Encryption or FHE for short is that it allows operations to be executed without the need of a secret key.[[36]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-36) FHE has been linked not only to cloud computing but to electronic voting as well. Fully Homomorphic Encryption has been especially helpful with the development of cloud computing and computing technologies. However, as these systems are developing the need for cloud security has also increased. FHE aims to secure data transmission as well as cloud computing storage with its encryption algorithms.[[37]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-37) Its goal is to be a much more secure and efficient method of encryption on a larger scale to handle the massive capabilities of the cloud.

### Searchable encryption (SE)**[[edit](https://en.wikipedia.org/w/index.php?title=Cloud_computing_security&action=edit&section=28" \o "Edit section: Searchable encryption (SE))]**

Searchable encryption is a cryptographic system that offers secure search functions over encrypted data.[[38]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Wang_et_al._2018-38)[[39]](https://en.wikipedia.org/wiki/Cloud_computing_security#cite_note-Naveed_2014-39) SE schemes can be classified into two categories: SE based on secret-key (or symmetric-key) cryptography, and SE based on public-key cryptography. In order to improve search efficiency, symmetric-key SE generally builds keyword indexes to answer user queries. This has the obvious disadvantage of providing multimodal access routes for unauthorized data retrieval, bypassing the encryption algorithm by subjecting the framework to alternative parameters within the shared cloud environmen

