**Cloud computing**, also **on-demand computing**, is a kind of Internet-based computing that provides shared processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources.[[1]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-2) Cloud computing and storage solutions provide users and enterprises with various capabilities to store and process their data in third-party [data centers](https://en.wikipedia.org/wiki/Data_center).[[3]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-cloudid-3) It relies on sharing of resources to achieve coherence and [economies of scale](https://en.wikipedia.org/wiki/Economies_of_scale), similar to a utility (like the [electricity grid](https://en.wikipedia.org/wiki/Electrical_grid)) over a network. At the foundation of cloud computing is the broader concept of [converged infrastructure](https://en.wikipedia.org/wiki/Converged_infrastructure) and [shared services](https://en.wikipedia.org/wiki/Shared_services).

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort.

Proponents claim that cloud computing allows companies to avoid upfront infrastructure costs, and focus on projects that differentiate their businesses instead of on infrastructure.[[4]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-aws.amazon-4) Proponents also claim that cloud computing allows enterprises to get their applications up and running faster, with improved manageability and less maintenance, and enables IT to more rapidly adjust resources to meet fluctuating and unpredictable business demand.[[4]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-aws.amazon-4)[[5]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-5)[[6]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-6) Cloud providers typically use a "pay as you go" model. This can lead to unexpectedly high charges if administrators do not adapt to the cloud pricing model.[[7]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-7)

The present availability of high-capacity networks, low-cost computers and storage devices as well as the widespread adoption of [hardware virtualization](https://en.wikipedia.org/wiki/Hardware_virtualization), [service-oriented architecture](https://en.wikipedia.org/wiki/Service-oriented_architecture), and [autonomic](https://en.wikipedia.org/wiki/Autonomic_Computing) and utility computing have led to a growth in cloud computing.[[8]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-8)[[9]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-gartner-9)[[10]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-really-10) Companies can scale up as computing needs increase and then scale down again as demands decrease.

Cloud computing has become a highly demanded service or utility due to the advantages of high computing power, cheap cost of services, high performance, scalability, accessibility as well as availability. Some cloud vendors are experiencing growth rates of 50% per annum,[[11]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-11) but due to being in a stage of infancy, it still has pitfalls that need proper attention to make cloud computing services more reliable and user friendly.

## History of cloud computing

### Origin of the term

The origin of the term *cloud computing* is unclear. The word "cloud" is commonly used in science to describe a large agglomeration of objects that visually appear from a distance as a cloud and describes any set of things whose details are not inspected further in a given context.[[14]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-14) Another explanation is that the old programs that drew network schematics surrounded the icons for servers with a circle, and a cluster of servers in a network diagram had several overlapping circles, which resembled a cloud.[[15]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-15)

In analogy to above usage the word *cloud* was used as a metaphor for the Internet and a standardized cloud-like shape was used to denote a network on telephony schematics and later to depict the Internet in [computer network diagrams](https://en.wikipedia.org/wiki/Computer_network_diagram). With this simplification, the implication is that the specifics of how the end points of a network are connected are not relevant for the purposes of understanding the diagram. The cloud symbol was used to represent networks of computing equipment in the original [ARPANET](https://en.wikipedia.org/wiki/ARPANET) by as early as 1977,[[16]](https://en.wikipedia.org/wiki/Cloud_computing" \l "cite_note-16) and the [CSNET](https://en.wikipedia.org/wiki/CSNET) by 1981[[17]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-17)—both predecessors to the Internet itself.

The term *cloud* has been used to refer to platforms for [distributed computing](https://en.wikipedia.org/wiki/Distributed_computing). In [*Wired's*](https://en.wikipedia.org/wiki/Wired_%28magazine%29) April 1994 feature "Bill and Andy's Excellent Adventure II" on the [Apple](https://en.wikipedia.org/wiki/Apple_Inc.) spin-off [General Magic](https://en.wikipedia.org/wiki/General_Magic), [Andy Hertzfeld](https://en.wikipedia.org/wiki/Andy_Hertzfeld) comments on General Magic's distributed programming language [Telescript](https://en.wikipedia.org/wiki/Telescript_%28programming_language%29) that:

"The beauty of Telescript ... is that now, instead of just having a device to program, we now have the entire Cloud out there, where a single program can go and travel to many different sources of information and create sort of a virtual service. No one had conceived that before. The example Jim White [the designer of Telescript, [X.400](https://en.wikipedia.org/wiki/X.400) and [ASN.1](https://en.wikipedia.org/wiki/ASN.1)] uses now is a date-arranging service where a software agent goes to the flower store and orders flowers and then goes to the ticket shop and gets the tickets for the show, and everything is communicated to both parties."

### The 1970s

During the mid-1970s, Time-sharing was popularly known as RJE ([Remote Job Entry](https://en.wikipedia.org/wiki/Remote_Job_Entry));[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] this terminology was mostly associated with large vendors such as [IBM](https://en.wikipedia.org/wiki/IBM) and [DEC](https://en.wikipedia.org/wiki/Digital_Equipment_Corporation).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] IBM developed the [VM Operating System](https://en.wikipedia.org/wiki/VM_%28operating_system%29) (first released in 1972) to provide time-sharing services[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] via [virtual machines](https://en.wikipedia.org/wiki/Virtual_machine).

### The 1990s

In the 1990s, telecommunications companies, who previously offered primarily dedicated point-to-point data circuits, began offering [virtual private network](https://en.wikipedia.org/wiki/Virtual_private_network) (VPN) services with comparable quality of service, but at a lower cost. By switching traffic as they saw fit to balance server use, they could use overall network bandwidth more effectively.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] They began to use the cloud symbol to denote the demarcation point between what the provider was responsible for and what users were responsible for. Cloud computing extends this boundary to cover all servers as well as the network infrastructure.[[21]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-21)

As computers became more prevalent, scientists and technologists explored ways to make large-scale computing power available to more users through time-sharing.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] They experimented with algorithms to optimize the infrastructure, platform, and applications to prioritize CPUs and increase efficiency for end users.[[22]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-MITCorbato-22)

### The New Millennium: 2000s

Since 2000, cloud computing has come into existence. In early 2008, [NASA](https://en.wikipedia.org/wiki/NASA)'s [OpenNebula](https://en.wikipedia.org/wiki/OpenNebula), enhanced in the RESERVOIR European Commission-funded project, became the first open-source software for deploying private and hybrid clouds, and for the federation of clouds.[[23]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-23) In the same year, efforts were focused on providing [quality of service](https://en.wikipedia.org/wiki/Quality_of_service) guarantees (as required by real-time interactive applications) to cloud-based infrastructures, in the framework of the IRMOS European Commission-funded project, resulting in a real-time cloud environment.[[24]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-24)[[25]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-Gogouvitis2012-25) By mid-2008, Gartner saw an opportunity for cloud computing "to shape the relationship among consumers of IT services, those who use IT services and those who sell them"[[26]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-26) and observed that "organizations are switching from company-owned hardware and software assets to per-use service-based models" so that the "projected shift to computing ... will result in dramatic growth in IT products in some areas and significant reductions in other areas."[[27]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-27)

[Microsoft Azure](https://en.wikipedia.org/wiki/Microsoft_Azure) was announced as "Azure" in October 2008 and released on 1 February 2010 as Windows Azure, before being renamed to Microsoft Azure on 25 March 2014.[[28]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-avail-28) For a time, Azure was on the [TOP500](https://en.wikipedia.org/wiki/TOP500) supercomputer list, before it dropped off it.[[29]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-29)

In July 2010, [Rackspace Hosting](https://en.wikipedia.org/wiki/Rackspace) and [NASA](https://en.wikipedia.org/wiki/NASA) jointly launched an open-source cloud-software initiative known as [OpenStack](https://en.wikipedia.org/wiki/OpenStack). The OpenStack project intended to help organizations offer cloud-computing services running on standard hardware. The early code came from NASA's [Nebula platform](https://en.wikipedia.org/wiki/Nebula_%28computing_platform%29) as well as from [Rackspace's Cloud Files](https://en.wikipedia.org/wiki/Rackspace_Cloud#Cloud_Files) platform.

On March 1, 2011, IBM announced the [IBM SmartCloud](https://en.wikipedia.org/wiki/IBM_cloud_computing#IBM_SmartCloud) framework to support [Smarter Planet](https://en.wikipedia.org/wiki/Smarter_Planet).[[30]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-30) Among the various components of the [Smarter Computing](https://en.wikipedia.org/w/index.php?title=Smarter_Computing&action=edit&redlink=1) foundation, cloud computing is a critical piece.

On June 7, 2012, Oracle announced the [Oracle Cloud](https://en.wikipedia.org/wiki/Oracle_Corporation#Services).[[31]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-31) While aspects of the Oracle Cloud are still in development, this cloud offering is poised to be the first to provide users with access to an integrated set of IT solutions, including the Applications ([SaaS](https://en.wikipedia.org/wiki/SaaS" \o "SaaS)), Platform ([PaaS](https://en.wikipedia.org/wiki/PaaS" \o "PaaS)), and Infrastructure ([IaaS](https://en.wikipedia.org/wiki/IaaS" \o "IaaS)) layers.

**Similar concepts**

Cloud computing is the result of the evolution and adoption of existing technologies and paradigms. The goal of cloud computing is to allow users to take beneﬁt from all of these technologies, without the need for deep knowledge about or expertise with each one of them. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles.[[35]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-HAM2012-35)

The main enabling technology for cloud computing is [virtualization](https://en.wikipedia.org/wiki/Virtualization). Virtualization software separates a physical computing device into one or more "virtual" devices, each of which can be easily used and managed to perform computing tasks. With [operating system–level virtualization](https://en.wikipedia.org/wiki/Operating_system%E2%80%93level_virtualization) essentially creating a scalable system of multiple independent computing devices, idle computing resources can be allocated and used more efficiently. Virtualization provides the agility required to speed up IT operations, and reduces cost by increasing infrastructure [utilization](https://en.wikipedia.org/wiki/Utilization). Autonomic computing automates the process through which the user can provision resources [on-demand](https://en.wikipedia.org/wiki/Code_on_demand). By minimizing user involvement, automation speeds up the process, reduces labor costs and reduces the possibility of human errors.[[35]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-HAM2012-35)

Users routinely face difficult business problems. Cloud computing adopts concepts from [Service-oriented Architecture](https://en.wikipedia.org/wiki/Service-oriented_Architecture) (SOA) that can help the user break these problems into [services](https://en.wikipedia.org/wiki/Service_%28systems_architecture%29) that can be integrated to provide a solution. Cloud computing provides all of its resources as services, and makes use of the well-established standards and best practices gained in the domain of SOA to allow global and easy access to cloud services in a standardized way.

Cloud computing also leverages concepts from utility computing to provide [metrics](https://en.wikipedia.org/wiki/Performance_metric) for the services used. Such metrics are at the core of the public cloud pay-per-use models. In addition, measured services are an essential part of the feedback loop in autonomic computing, allowing services to scale on-demand and to perform automatic failure recovery.

Cloud computing is a kind of [grid computing](https://en.wikipedia.org/wiki/Grid_computing); it has evolved by addressing the QoS (quality of service) and [reliability](https://en.wikipedia.org/wiki/Reliability_%28computer_networking%29) problems. Cloud computing provides the tools and technologies to build data/compute intensive parallel applications with much more affordable prices compared to traditional [parallel computing](https://en.wikipedia.org/wiki/Parallel_computing) techniques.[[35]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-HAM2012-35)

Cloud computing shares characteristics with:

* [Client–server model](https://en.wikipedia.org/wiki/Client%E2%80%93server_model)—*Client–server computing* refers broadly to any [distributed application](https://en.wikipedia.org/wiki/Distributed_application) that distinguishes between service providers (servers) and service requestors (clients).[[36]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-36)
* [Grid computing](https://en.wikipedia.org/wiki/Grid_computing)—"A form of distributed and parallel computing, whereby a 'super and virtual computer' is composed of a [cluster](https://en.wikipedia.org/wiki/Cluster_%28computing%29) of networked, [loosely coupled](https://en.wikipedia.org/wiki/Loose_coupling) computers acting in concert to perform very large tasks."
* [Fog computing](https://en.wikipedia.org/wiki/Fog_computing)—Distributed computing paradigm that provides data, compute, storage and application services closer to client or near-user edge devices, such as network routers. Furthermore, fog computing handles data at the network level, on smart devices and on the end-user client side (e.g. mobile devices), instead of sending data to a remote location for processing.
* [Dew computing](https://en.wikipedia.org/w/index.php?title=Dew_computing&action=edit&redlink=1)—In the existing computing hierarchy, the Dew computing is positioned as the ground level for the cloud and fog computing paradigms. Compared to fog computing, which supports emerging IoT applications that demand real-time and predictable latency and the dynamic network reconfigurability, Dew computing pushes the frontiers to computing applications, data, and low level services away from centralized virtual nodes to the end users.[[37]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-skala-37)
* [Mainframe computer](https://en.wikipedia.org/wiki/Mainframe_computer)—Powerful computers used mainly by large organizations for critical applications, typically bulk data processing such as: [census](https://en.wikipedia.org/wiki/Census); industry and consumer statistics; police and secret intelligence services; [enterprise resource planning](https://en.wikipedia.org/wiki/Enterprise_resource_planning); and financial [transaction processing](https://en.wikipedia.org/wiki/Transaction_processing).
* [Utility computing](https://en.wikipedia.org/wiki/Utility_computing)—The "packaging of [computing resources](https://en.wikipedia.org/wiki/Computational_resource), such as computation and storage, as a metered service similar to a traditional public utility, such as electricity."[[38]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-It.27s_you.27ve-38)[[39]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-39)
* [Peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer)—A distributed architecture without the need for central coordination. Participants are both suppliers and consumers of resources (in contrast to the traditional client–server model).

**Characteristics**

Cloud computing exhibits the following key characteristics:

* **Agility** improves with users' ability to re-provision technological infrastructure resources.
* **Cost** reductions claimed by cloud providers. A public-cloud delivery model converts capital expenditure to [operational expenditure](https://en.wikipedia.org/wiki/Operational_expenditure).[[40]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-40) This purportedly lowers [barriers to entry](https://en.wikipedia.org/wiki/Barriers_to_entry), as infrastructure is typically provided by a third party and need not be purchased for one-time or infrequent intensive computing tasks. Pricing on a utility computing basis is fine-grained, with usage-based options and fewer IT skills are required for implementation (in-house).[[41]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-idc-41) The e-FISCAL project's state-of-the-art repository[[42]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-42) contains several articles looking into cost aspects in more detail, most of them concluding that costs savings depend on the type of activities supported and the type of infrastructure available in-house.
* [**Device and location independence**](https://en.wikipedia.org/wiki/Device_independence)[[43]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-yarmis-43) enable users to access systems using a web browser regardless of their location or what device they use (e.g., PC, mobile phone). As infrastructure is off-site (typically provided by a third-party) and accessed via the Internet, users can connect from anywhere.[[41]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-idc-41)
* [**Maintenance**](https://en.wikipedia.org/wiki/Software_maintenance) of cloud computing applications is easier, because they do not need to be installed on each user's computer and can be accessed from different places.
* [**Multitenancy**](https://en.wikipedia.org/wiki/Multitenancy) enables sharing of resources and costs across a large pool of users thus allowing for:
  + **centralization** of infrastructure in locations with lower costs (such as real estate, electricity, etc.)
  + **peak-load capacity** increases (users need not engineer for highest possible load-levels)
  + **utilisation and efficiency** improvements for systems that are often only 10–20% utilised.[[44]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-amazon-44)[[45]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-45)
* [**Performance**](https://en.wikipedia.org/wiki/Computer_performance) is monitored, and consistent and loosely coupled architectures are constructed using [web services](https://en.wikipedia.org/wiki/Web_services) as the system interface.[[41]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-idc-41)[[46]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-46)[[47]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-Elsevier.com-47)
* [**Productivity**](https://en.wikipedia.org/wiki/Productivity) may be increased when multiple users can work on the same data simultaneously, rather than waiting for it to be saved and emailed. Time may be saved as information does not need to be re-entered when fields are matched, nor do users need to install application software upgrades to their computer.[[48]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-Smith2013-48)
* **Reliability** improves with the use of multiple redundant sites, which makes well-designed cloud computing suitable for [business continuity](https://en.wikipedia.org/wiki/Business_continuity) and [disaster recovery](https://en.wikipedia.org/wiki/Disaster_recovery).[[49]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-49)
* **Scalability and** [**elasticity**](https://en.wikipedia.org/wiki/Elasticity_%28cloud_computing%29) via dynamic ("on-demand") [provisioning](https://en.wikipedia.org/wiki/Provisioning) of resources on a fine-grained, self-service basis in near real-time[[50]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-vmstartuptime2012-50)[[51]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-51) (Note, the VM startup time varies by VM type, location, OS and cloud providers[[50]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-vmstartuptime2012-50)), without users having to engineer for peak loads.[[52]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-52)[[53]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-53)[[54]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-He_15.E2.80.9322-54) This gives the ability to scale up when the usage need increases or down if resources are not being used.[[55]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-55)
* [**Security**](https://en.wikipedia.org/wiki/Computer_security) can improve due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers are able to devote resources to solving security issues that many customers cannot afford to tackle.[[56]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-56) However, the complexity of security is greatly increased when data is distributed over a wider area or over a greater number of devices, as well as in multi-tenant systems shared by unrelated users. In addition, user access to security [audit logs](https://en.wikipedia.org/wiki/Audit_log) may be difficult or impossible. Private cloud installations are in part motivated by users' desire to retain control over the infrastructure and avoid losing control of information security.

The [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology)'s definition of cloud computing identifies "five essential characteristics":

*On-demand self-service.* A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

*Broad network access.* Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

*Resource pooling.* The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

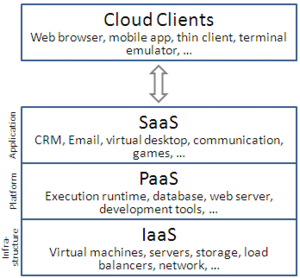
*Rapid elasticity.* Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.

*Measured service.* Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

*— National Institute of Standards and Technology[[57]](https://en.wikipedia.org/wiki/Cloud_computing" \l "cite_note-nist-57)*

**Service models**

Though [service-oriented architecture](https://en.wikipedia.org/wiki/Service-oriented_architecture) advocates "everything as a service" (with the acronyms **EaaS** or **XaaS** or simply [**aas**](https://en.wikipedia.org/wiki/As_a_service)),[[58]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-58) cloud-computing providers offer their "services" according to different models,[[57]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-nist-57)[[59]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-Buyya-59)[[*need quotation to verify*](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)] which happen to form a [stack](https://en.wikipedia.org/wiki/Solution_stack): infrastructure-, platform- and software-as-a-service.[[60]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-60)

[](https://en.wikipedia.org/wiki/File:Cloud_computing_layers.png)

Cloud-computing layers accessible within a stack

**Infrastructure as a service (IaaS)**

See also: [Category:Cloud infrastructure](https://en.wikipedia.org/wiki/Category:Cloud_infrastructure)

In the most basic cloud-service model—and according to the IETF (Internet Engineering Task Force)—providers of IaaS offer computers—physical or (more often) virtual machines—and other resources. IaaS refers to online services that abstract the user from the details of infrastructure like physical computing resources, location, data partitioning, scaling, security, backup etc. A [hypervisor](https://en.wikipedia.org/wiki/Hypervisor), such as [Xen](https://en.wikipedia.org/wiki/Xen), [Oracle VirtualBox](https://en.wikipedia.org/wiki/VirtualBox), [KVM](https://en.wikipedia.org/wiki/Kernel-based_Virtual_Machine), [VMware ESX/ESXi](https://en.wikipedia.org/wiki/VMware_ESX), or [Hyper-V](https://en.wikipedia.org/wiki/Hyper-V) runs the virtual machines as guests. Pools of hypervisors within the cloud operational system can support large numbers of virtual machines and the ability to scale services up and down according to customers' varying requirements. IaaS clouds often offer additional resources such as a virtual-machine [disk-image](https://en.wikipedia.org/wiki/Disk_image) library, raw [block storage](https://en.wikipedia.org/wiki/Block_storage), file or [object storage](https://en.wikipedia.org/wiki/Object_storage), firewalls, load balancers, IP addresses, [virtual local area networks](https://en.wikipedia.org/wiki/VLAN) (VLANs), and software bundles.[[61]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-DHAC-61) IaaS-cloud providers supply these resources on-demand from their large pools of equipment installed in [data centers](https://en.wikipedia.org/wiki/Data_centers). For [wide-area](https://en.wikipedia.org/wiki/Wide_area_network) connectivity, customers can use either the Internet or [carrier clouds](https://en.wikipedia.org/wiki/Carrier_cloud) (dedicated [virtual private networks](https://en.wikipedia.org/wiki/Virtual_private_network)).

To deploy their applications, cloud users install operating-system images and their application software on the cloud infrastructure.[[62]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-62)[[*unreliable source?*](https://en.wikipedia.org/wiki/Wikipedia:Identifying_reliable_sources)] In this model, the cloud user patches and maintains the operating systems and the application software. Cloud providers typically bill IaaS services on a utility computing basis: cost reflects the amount of resources allocated and consumed.[[63]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-63)[[64]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-64)[[65]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-65)[[66]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-66)

**Platform as a service (PaaS)**

Main article: [Platform as a service](https://en.wikipedia.org/wiki/Platform_as_a_service)

See also: [Category:Cloud platforms](https://en.wikipedia.org/wiki/Category:Cloud_platforms)

PaaS vendors offer a development environment to application developers. The provider typically develops toolkit and standards for development and channels for distribution and payment. In the PaaS models, cloud providers deliver a [computing platform](https://en.wikipedia.org/wiki/Computing_platform), typically including operating system, programming-language execution environment, database, and web server. Application developers can develop and run their software solutions on a cloud platform without the cost and complexity of buying and managing the underlying hardware and software layers. With some PaaS offers like [Microsoft Azure](https://en.wikipedia.org/wiki/Microsoft_Azure) and [Google App Engine](https://en.wikipedia.org/wiki/Google_App_Engine), the underlying computer and storage resources scale automatically to match application demand so that the cloud user does not have to allocate resources manually. The latter has also been proposed by an architecture aiming to facilitate real-time in cloud environments.[[67]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-67)[[*need quotation to verify*](https://en.wikipedia.org/wiki/Wikipedia:Verifiability)] Even more specific application types can be provided via PaaS, such as media encoding as provided by services like bitcodin.com[[68]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-68) or media.io.[[69]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-69)

Some integration and data management providers have also embraced specialized applications of PaaS as delivery models for data solutions. Examples include **iPaaS** and **dPaaS**. iPaaS (Integration Platform as a Service) enables customers to develop, execute and govern integration flows.[[70]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-GartnerGlossary-70) Under the iPaaS integration model, customers drive the development and deployment of integrations without installing or managing any hardware or middleware.[[71]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-GartnerReferenceModel-71) dPaaS (Data Platform as a Service) delivers integration—and data-management—products as a fully managed service.[[72]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-ITBusinessEdge-72) Under the dPaaS model, the PaaS provider, not the customer, manages the development and execution of data solutions by building tailored data applications for the customer. dPaaS users retain transparency and control over data through [data-visualization](https://en.wikipedia.org/wiki/Data_visualization) tools.[[73]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-EnterpriseCIOForum-73)

Platform as a Service (PaaS) consumers do not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but have control over the deployed applications and possibly configuration settings for the application-hosting environment.

**Software as a service (SaaS)**

Main article: [Software as a service](https://en.wikipedia.org/wiki/Software_as_a_service)

In the software as a service (SaaS) model, users gain access to application software and databases. Cloud providers manage the infrastructure and platforms that run the applications. SaaS is sometimes referred to as "on-demand software" and is usually priced on a pay-per-use basis or using a subscription fee.[*[citation needed](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "Wikipedia:Citation needed)*]

In the SaaS model, cloud providers install and operate application software in the cloud and cloud users access the software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs. This eliminates the need to install and run the application on the cloud user's own computers, which simplifies maintenance and support. Cloud applications differ from other applications in their scalability—which can be achieved by cloning tasks onto multiple [virtual machines](https://en.wikipedia.org/wiki/Virtual_machines) at run-time to meet changing work demand.[[74]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-hamdaqa-74) [Load balancers](https://en.wikipedia.org/wiki/Load_balancer) distribute the work over the set of virtual machines. This process is transparent to the cloud user, who sees only a single access-point. To accommodate a large number of cloud users, cloud applications can be [*multitenant*](https://en.wikipedia.org/wiki/Multitenant), meaning that any machine may serve more than one cloud-user organization.

The pricing model for SaaS applications is typically a monthly or yearly flat fee per user,[[75]](https://en.wikipedia.org/wiki/Cloud_computing" \l "cite_note-Chou-75) so prices become scalable and adjustable if users are added or removed at any point.[[76]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-76)

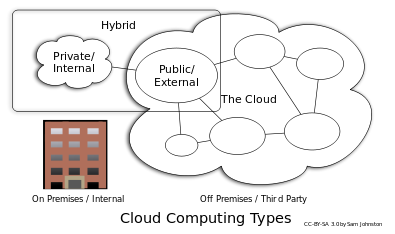
Proponents claim that SaaS gives a [business](https://en.wikipedia.org/wiki/Business) the potential to reduce IT operational costs by outsourcing hardware and software maintenance and support to the cloud provider. This enables the business to reallocate IT operations costs away from hardware/software spending and from personnel expenses, towards meeting other goals. In addition, with applications hosted centrally, updates can be released without the need for users to install new software. One drawback of SaaS comes with storing the users' data on the cloud provider's server. As a result,[*[citation needed](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "Wikipedia:Citation needed)*] there could be unauthorized access to the data. For this reason, users are increasingly[*[quantify](https://en.wikipedia.org/wiki/Wikipedia:Manual_of_Style/Dates_and_numbers" \o "Wikipedia:Manual of Style/Dates and numbers)*] adopting intelligent third-party [key-management](https://en.wikipedia.org/wiki/Key_management) systems to help secure their data.[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

**Cloud clients**

See also: [Category:Cloud clients](https://en.wikipedia.org/wiki/Category:Cloud_clients) and [Cloud API](https://en.wikipedia.org/wiki/Cloud_API)

Users access cloud computing using networked client devices, such as [desktop computers](https://en.wikipedia.org/wiki/Desktop_computers), [laptops](https://en.wikipedia.org/wiki/Laptop), [tablets](https://en.wikipedia.org/wiki/Tablet_computer) and [smartphones](https://en.wikipedia.org/wiki/Smartphones) and any Ethernet enabled device such as Home Automation Gadgets. Some of these devices—*cloud clients*—rely on cloud computing for all or a majority of their applications so as to be essentially useless without it. Examples are [thin clients](https://en.wikipedia.org/wiki/Thin_clients) and the browser-based [Chromebook](https://en.wikipedia.org/wiki/Chromebook). Many cloud applications do not require specific software on the client and instead use a web browser to interact with the cloud application. With [Ajax](https://en.wikipedia.org/wiki/Ajax_%28programming%29) and [HTML5](https://en.wikipedia.org/wiki/HTML5) these [Web user interfaces](https://en.wikipedia.org/wiki/Web_user_interface) can achieve a similar, or even better, [look and feel](https://en.wikipedia.org/wiki/Look_and_feel) to native applications. Some cloud applications, however, support specific client software dedicated to these applications (e.g., [virtual desktop](https://en.wikipedia.org/wiki/Desktop_virtualization) clients and most email clients). Some legacy applications (line of business applications that until now have been prevalent in thin client computing) are delivered via a screen-sharing technology.

**Deployment models**

[](https://en.wikipedia.org/wiki/File:Cloud_computing_types.svg)

Cloud computing types

**Private cloud**

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party, and hosted either internally or externally.[[57]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-nist-57) Undertaking a private cloud project requires a significant level and degree of engagement to virtualize the business environment, and requires the organization to reevaluate decisions about existing resources. When done right, it can improve business, but every step in the project raises security issues that must be addressed to prevent serious vulnerabilities. Self-run data centers[[77]](https://en.wikipedia.org/wiki/Cloud_computing" \l "cite_note-77) are generally capital intensive. They have a significant physical footprint, requiring allocations of space, hardware, and environmental controls. These assets have to be refreshed periodically, resulting in additional capital expenditures. They have attracted criticism because users "still have to buy, build, and manage them" and thus do not benefit from less hands-on management,[[78]](https://en.wikipedia.org/wiki/Cloud_computing" \l "cite_note-iwpc-78) essentially "[lacking] the economic model that makes cloud computing such an intriguing concept".[[79]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-79)[[80]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-80)

**Public cloud**

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use. Public cloud services may be free.[[81]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-81) Technically there may be little or no difference between public and private cloud architecture, however, security consideration may be substantially different for services (applications, storage, and other resources) that are made available by a service provider for a public audience and when communication is effected over a non-trusted network. Generally, public cloud service providers like Amazon AWS, Microsoft and Google own and operate the infrastructure at their [data center](https://en.wikipedia.org/wiki/Data_center) and access is generally via the Internet. AWS and Microsoft also offer direct connect services called "AWS Direct Connect" and "Azure ExpressRoute" respectively, such connections require customers to purchase or lease a private connection to a peering point offered by the cloud provider.[[41]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-idc-41)

**Hybrid cloud**

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.[[57]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-nist-57)

[Gartner, Inc.](https://en.wikipedia.org/wiki/Gartner) defines a hybrid cloud service as a cloud computing service that is composed of some combination of private, public and community cloud services, from different service providers.[[82]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-82) A hybrid cloud service crosses isolation and provider boundaries so that it can't be simply put in one category of private, public, or community cloud service. It allows one to extend either the capacity or the capability of a cloud service, by aggregation, integration or customization with another cloud service.

Varied use cases for hybrid cloud composition exist. For example, an organization may store sensitive client data in house on a private cloud application, but interconnect that application to a business intelligence application provided on a public cloud as a software service.[[83]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-83) This example of hybrid cloud extends the capabilities of the enterprise to deliver a specific business service through the addition of externally available public cloud services. Hybrid cloud adoption depends on a number of factors such as data security and compliance requirements, level of control needed over data, and the applications an organization uses.[[84]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-84)

Another example of hybrid cloud is one where [IT](https://en.wikipedia.org/wiki/Information_technology) organizations use public cloud computing resources to meet temporary capacity needs that can not be met by the private cloud.[[85]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-85) This capability enables hybrid clouds to employ cloud bursting for scaling across clouds.[[57]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-nist-57) Cloud bursting is an application deployment model in which an application runs in a private cloud or data center and "bursts" to a public cloud when the demand for computing capacity increases. A primary advantage of cloud bursting and a hybrid cloud model is that an organization only pays for extra compute resources when they are needed.[[86]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-86) Cloud bursting enables data centers to create an in-house IT infrastructure that supports average workloads, and use cloud resources from public or private clouds, during spikes in processing demands.[[87]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-87)

The specialized model of hybrid cloud, which is built atop heterogeneous hardware, is called "Cross-platform Hybrid Cloud". A cross-platform hybrid cloud is usually powered by different CPU architectures, for example, x86-64 and ARM, underneath. Users can transparently deploy and scale applications without knowledge of the cloud's hardware diversity.[[88]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-88) This kind of cloud emerges from the raise of ARM-based system-on-chip for server-class computing.

**Others**

**Community cloud**

[Community cloud](https://en.wikipedia.org/wiki/Community_cloud) shares infrastructure between several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), whether managed internally or by a third-party, and either hosted internally or externally. The costs are spread over fewer users than a public cloud (but more than a private cloud), so only some of the cost savings potential of cloud computing are realized.[[57]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-nist-57)

**Distributed cloud**

A cloud computing platform can be assembled from a distributed set of machines in different locations, connected to a single network or hub service. It is possible to distinguish between two types of distributed clouds: public-resource computing and volunteer cloud.

* **Public-resource computing**—This type of distributed cloud results from an expansive definition of cloud computing, because they are more akin to distributed computing than cloud computing. Nonetheless, it is considered a sub-class of cloud computing, and some examples include distributed computing platforms such as [BOINC](https://en.wikipedia.org/wiki/BOINC) and [Folding@Home](https://en.wikipedia.org/wiki/Folding@Home).
* **Volunteer cloud**—Volunteer cloud computing is characterized as the intersection of public-resource computing and cloud computing, where a cloud computing infrastructure is built using volunteered resources. Many challenges arise from this type of infrastructure, because of the volatility of the resources used to built it and the dynamic environment it operates in. It can also be called peer-to-peer clouds, or ad-hoc clouds. An interesting effort in such direction is Cloud@Home, it aims to implement a cloud computing infrastructure using volunteered resources providing a business-model to incentivize contributions through financial restitution.[[89]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-89)

**Intercloud**

Main article: [Intercloud](https://en.wikipedia.org/wiki/Intercloud)

The [Intercloud](https://en.wikipedia.org/wiki/Intercloud)[[90]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-90) is an interconnected global "cloud of clouds"[[91]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-kk-91)[[92]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-92) and an extension of the Internet "network of networks" on which it is based. The focus is on direct [interoperability](https://en.wikipedia.org/wiki/Interoperability) between public cloud service providers, more so than between providers and consumers (as is the case for hybrid- and multi-cloud).[[93]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-93)[[94]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-94)[[95]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-95)

**Multicloud**

Main article: [Multicloud](https://en.wikipedia.org/wiki/Multicloud)

Multicloud is the use of multiple cloud computing services in a single heterogeneous architecture to reduce reliance on single vendors, increase flexibility through choice, mitigate against disasters, etc. It differs from hybrid cloud in that it refers to multiple cloud services, rather than multiple deployment modes (public, private, legacy).

**Security and privacy**

Main article: [Cloud computing issues](https://en.wikipedia.org/wiki/Cloud_computing_issues)

Cloud computing poses privacy concerns because the service provider can access the data that is in the cloud at any time. It could accidentally or deliberately alter or even delete information.[[100]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-ryan-100) Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies, which users must agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored.[[100]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-ryan-100) Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.[[3]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-cloudid-3)[[100]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-ryan-100)

According to the [Cloud Security Alliance](https://en.wikipedia.org/wiki/Cloud_Security_Alliance), the top three threats in the cloud are *Insecure Interfaces and API's*, *Data Loss & Leakage*, and *Hardware Failure*—which accounted for 29%, 25% and 10% of all cloud security outages respectively. Together, these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server. Therefore, Information leakage may arise by mistake when information for one customer is given to other.[[101]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-101) Additionally, [Eugene Schultz](https://en.wikipedia.org/wiki/Eugene_Schultz), chief technology officer at Emagined Security, said that hackers are spending substantial time and effort looking for ways to penetrate the cloud. "There are some real Achilles' heels in the cloud infrastructure that are making big holes for the bad guys to get into". Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack—a process he called "hyperjacking". Some examples of this include the Dropbox security breach, and iCloud 2014 leak.[[102]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-psg.hitachi-solutions.com-102) Dropbox had been breached in October 2014, having over 7 million of its users passwords stolen by hackers in an effort to get monetary value from it by Bitcoins (BTC). By having these passwords, they are able to read private data as well as have this data be indexed by search engines (making the information public).[[102]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-psg.hitachi-solutions.com-102)

There is the problem of legal ownership of the data (If a user stores some data in the cloud, can the cloud provider profit from it?). Many Terms of Service agreements are silent on the question of ownership.[[103]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-103)

Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services.[[104]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-104) Some small businesses that don't have expertise in [IT](https://en.wikipedia.org/wiki/Information_technology) security could find that it's more secure for them to use a public cloud.

There is the risk that end users don't understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading). This is important now that cloud computing is becoming popular and required for some services to work, for example for an [intelligent personal assistant](https://en.wikipedia.org/wiki/Intelligent_personal_assistant) (Apple's [Siri](https://en.wikipedia.org/wiki/Siri) or [Google Now](https://en.wikipedia.org/wiki/Google_Now)).

Fundamentally private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.

## The future

Cloud computing is therefore still as much a research topic, as it is a market offering.[[107]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-ghc-107) What is clear through the evolution of cloud computing services is that the chief technical officer (CTO) is a major driving force behind cloud adoption.[[108]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-108) The major cloud technology developers continue to invest billions a year in cloud R&D; for example: in 2011 Microsoft committed 90% of its US$9.6bn [R&D](https://en.wikipedia.org/wiki/Research_and_development) budget to its cloud.[[109]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-109) Centaur Partners also predict that SaaS revenue will grow from US$13.5B in 2011 to $32.8B in 2016.[[110]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-110) This expansion also includes Finance and Accounting SaaS.[[111]](https://en.wikipedia.org/wiki/Cloud_computing#cite_note-111) Additionally, more industries are turning to cloud technology as an efficient way to improve quality services due to its capabilities to reduce overhead costs, downtime, and automate infrastructure deployment

# Multicloud

From Wikipedia, the free encyclopedia

**Multicloud** is the use of multiple [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) services in a single heterogeneous architecture.

For example, an enterprise may concurrently use separate cloud providers for infrastructure (IaaS) and software (SaaS) services, or use multiple infrastructure (IaaS) providers. In the latter case, they may use different infrastructure providers for different workloads, deploy a single workload load balanced across multiple providers (active-active), or deploy a single workload on one provider, with a backup on another (active-passive).

There are a number of reasons for deploying a multicloud architecture, including reducing reliance on any single vendor, increasing flexibility through choice, mitigating against disasters, etc. It is similar to the use of best-of-breed applications from multiple developers on a personal computer, rather than the defaults offered by the operating system vendor. It is a recognition of the fact that no one provider can be everything for everyone. It differs from hybrid cloud in that it refers to multiple cloud services rather than multiple deployment modes (public, private, legacy).[[1]](https://en.wikipedia.org/wiki/Multicloud#cite_note-rouse-1)[[2]](https://en.wikipedia.org/wiki/Multicloud#cite_note-king-2)

Various issues also present themselves in a multicloud environment. Security and governance is more complicated, and more "moving parts" may create resiliency issues. Selection of the right cloud products and services can also present a challenge, and users may suffer from the [paradox of choice](https://en.wikipedia.org/wiki/Paradox_of_choice).

**PHP**

**PHP** is a [server-side scripting](https://en.wikipedia.org/wiki/Server-side_scripting) language designed for [web development](https://en.wikipedia.org/wiki/Web_development) but also used as a [general-purpose programming language](https://en.wikipedia.org/wiki/General-purpose_programming_language). Originally created by [Rasmus Lerdorf](https://en.wikipedia.org/wiki/Rasmus_Lerdorf) in 1994,[[3]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-History_of_PHP-3) the PHP [reference implementation](https://en.wikipedia.org/wiki/Reference_implementation) is now produced by The PHP Group.[[4]](https://en.wikipedia.org/wiki/PHP#cite_note-about_PHP-4) PHP originally stood for *Personal Home Page*,[[3]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-History_of_PHP-3) but it now stands for the [recursive](https://en.wikipedia.org/wiki/Recursive_acronym) [backronym](https://en.wikipedia.org/wiki/Backronym) *PHP: Hypertext Preprocessor*.[[5]](https://en.wikipedia.org/wiki/PHP#cite_note-5)

PHP code may be embedded into [HTML](https://en.wikipedia.org/wiki/HTML) code, or it can be used in combination with various [web template systems](https://en.wikipedia.org/wiki/Web_template_system), web content management system and [web frameworks](https://en.wikipedia.org/wiki/Web_framework). PHP code is usually processed by a PHP [interpreter](https://en.wikipedia.org/wiki/Interpreter_%28computing%29) implemented as a [module](https://en.wikipedia.org/wiki/Plugin_%28computing%29) in the web server or as a [Common Gateway Interface](https://en.wikipedia.org/wiki/Common_Gateway_Interface) (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated web page. PHP code may also be executed with a [command-line interface](https://en.wikipedia.org/wiki/Command-line_interface) (CLI) and can be used to implement [standalone](https://en.wikipedia.org/wiki/Computer_software) [graphical applications](https://en.wikipedia.org/wiki/Graphical_user_interface).[[6]](https://en.wikipedia.org/wiki/PHP#cite_note-6)

The standard PHP interpreter, powered by the [Zend Engine](https://en.wikipedia.org/wiki/Zend_Engine), is [free software](https://en.wikipedia.org/wiki/Free_software) released under the [PHP License](https://en.wikipedia.org/wiki/PHP_License). PHP has been widely ported and can be deployed on most web servers on almost every [operating system](https://en.wikipedia.org/wiki/Operating_system) and [platform](https://en.wikipedia.org/wiki/Computing_platform), free of charge.[[7]](https://en.wikipedia.org/wiki/PHP#cite_note-foundations-7)

The PHP language evolved without a written [formal specification](https://en.wikipedia.org/wiki/Formal_specification) or standard until 2014, leaving the canonical PHP interpreter as a [*de facto*](https://en.wikipedia.org/wiki/De_facto) standard. Since 2014 work has gone on to create a formal PHP specification.

### PHP 5

On July 13, 2004, PHP 5 was released, powered by the new Zend Engine II.[[4]](https://en.wikipedia.org/wiki/PHP#cite_note-about_PHP-4) PHP 5 included new features such as improved support for [object-oriented programming](https://en.wikipedia.org/wiki/Object-oriented_programming), the PHP Data Objects (PDO) extension (which defines a lightweight and consistent interface for accessing databases), and numerous performance enhancements.[[22]](https://en.wikipedia.org/wiki/PHP#cite_note-22) In 2008 PHP 5 became the only stable version under development. [Late static binding](https://en.wikipedia.org/wiki/Late_static_binding) had been missing from PHP and was added in version 5.3.[[23]](https://en.wikipedia.org/wiki/PHP#cite_note-23)[[24]](https://en.wikipedia.org/wiki/PHP#cite_note-24)

Many high-profile open-source projects ceased to support PHP 4 in new code as of February 5, 2008, because of the GoPHP5 initiative,[[25]](https://en.wikipedia.org/wiki/PHP#cite_note-gophp5_projects-25) provided by a consortium of PHP developers promoting the transition from PHP 4 to PHP 5.[[26]](https://en.wikipedia.org/wiki/PHP#cite_note-gophp5-26)[[27]](https://en.wikipedia.org/wiki/PHP#cite_note-27)

Over time, PHP interpreters became available on most existing [32-bit](https://en.wikipedia.org/wiki/32-bit) and [64-bit](https://en.wikipedia.org/wiki/64-bit) operating systems, either by building them from the PHP source code, or by using pre-built binaries.[[28]](https://en.wikipedia.org/wiki/PHP#cite_note-28) For the PHP versions 5.3 and 5.4, the only available [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) binary distributions were 32-bit [x86](https://en.wikipedia.org/wiki/X86) builds,[[29]](https://en.wikipedia.org/wiki/PHP#cite_note-29)[[30]](https://en.wikipedia.org/wiki/PHP#cite_note-30) requiring Windows 32-bit compatibility mode while using [Internet Information Services](https://en.wikipedia.org/wiki/Internet_Information_Services) (IIS) on a 64-bit Windows platform. PHP version 5.5 made the 64-bit [x86-64](https://en.wikipedia.org/wiki/X86-64) builds available for Microsoft Windows.[[31]](https://en.wikipedia.org/wiki/PHP#cite_note-31)

### PHP 6 and Unicode

PHP received mixed reviews due to lacking native [Unicode](https://en.wikipedia.org/wiki/Unicode) support at the core language level.[[32]](https://en.wikipedia.org/wiki/PHP#cite_note-32)[[33]](https://en.wikipedia.org/wiki/PHP#cite_note-33) In 2005, a project headed by Andrei Zmievski was initiated to bring native Unicode support throughout PHP, by embedding the [International Components for Unicode](https://en.wikipedia.org/wiki/International_Components_for_Unicode) (ICU) library, and representing text strings as [UTF-16](https://en.wikipedia.org/wiki/UTF-16) internally.[[34]](https://en.wikipedia.org/wiki/PHP#cite_note-34) Since this would cause major changes both to the internals of the language and to user code, it was planned to release this as version 6.0 of the language, along with other major features then in development.[[35]](https://en.wikipedia.org/wiki/PHP#cite_note-35)

However, a shortage of developers who understood the necessary changes, and performance problems arising from conversion to and from UTF-16, which is rarely used in a web context, led to delays in the project.[[36]](https://en.wikipedia.org/wiki/PHP#cite_note-36) As a result, a PHP 5.3 release was created in 2009, with many non-Unicode features back-ported from PHP 6, notably namespaces. In March 2010, the project in its current form was officially abandoned, and a PHP 5.4 release was prepared containing most remaining non-Unicode features from PHP 6, such as traits and closure re-binding.[[37]](https://en.wikipedia.org/wiki/PHP#cite_note-37) Initial hopes were that a new plan would be formed for Unicode integration, but as of 2014 none has been adopted.

### PHP 7

During 2014 and 2015, a new major PHP version was developed, which was numbered PHP 7. The numbering of this version involved some debate.[[38]](https://en.wikipedia.org/wiki/PHP#cite_note-38) While the PHP 6 Unicode experiment had never been released, several articles and book titles referenced the PHP 6 name, which might have caused confusion if a new release were to reuse the name.[[39]](https://en.wikipedia.org/wiki/PHP#cite_note-39) After a vote, the name PHP 7 was chosen.[[40]](https://en.wikipedia.org/wiki/PHP#cite_note-40)

The foundation of PHP 7 is a PHP [branch](https://en.wikipedia.org/wiki/Branching_%28revision_control%29) that was originally dubbed *PHP next generation* (*phpng*). It was authored by Dmitry Stogov, Xinchen Hui and Nikita Popov,[[41]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-41) and aimed to optimize PHP performance by refactoring the Zend Engine while retaining near-complete language compatibility.[[42]](https://en.wikipedia.org/wiki/PHP#cite_note-42) As of 14 July 2014, [WordPress](https://en.wikipedia.org/wiki/WordPress)-based benchmarks, which served as the main benchmark suite for the phpng project, showed an almost 100% increase in performance. Changes from phpng are also expected to make it easier to improve performance in the future, as more compact data structures and other changes are seen as better suited for a successful migration to a [just-in-time](https://en.wikipedia.org/wiki/Just-in-time_compilation) (JIT) compiler.[[43]](https://en.wikipedia.org/wiki/PHP#cite_note-phpng-43) Because of the significant changes, the reworked Zend Engine is called *Zend Engine 3*, succeeding Zend Engine 2 used in PHP 5.[[44]](https://en.wikipedia.org/wiki/PHP#cite_note-ZE2-44)

Because of major internal changes in phpng, it must receive a new [major version](https://en.wikipedia.org/wiki/Software_versioning) number of PHP, rather than a minor PHP 5 release, according to PHP's release process.[[45]](https://en.wikipedia.org/wiki/PHP#cite_note-releaseprocess-45) Major versions of PHP are allowed to break backward-compatibility of code and therefore PHP 7 presented an opportunity for other improvements beyond phpng that require backward-compatibility breaks. In particular, it involved the following changes:

* Many fatal- or recoverable-level legacy PHP error mechanisms were replaced with modern object-oriented [exceptions](https://en.wikipedia.org/wiki/Exception_%28computer_science%29)[[46]](https://en.wikipedia.org/wiki/PHP#cite_note-engine_exceptions-46)
* The syntax for variable dereferencing was reworked to be internally more consistent and complete, allowing the use of the operators *->*, *[]*, *()*, *{}*, and *::* with arbitrary meaningful left-hand-side expressions[[47]](https://en.wikipedia.org/wiki/PHP#cite_note-uvs-47)
* Support for legacy PHP 4-style constructor methods was removed[[48]](https://en.wikipedia.org/wiki/PHP#cite_note-48)
* The behavior of the [*foreach* statement](https://en.wikipedia.org/wiki/Foreach_loop) was changed to be more predictable[[49]](https://en.wikipedia.org/wiki/PHP#cite_note-49)
* Constructors for the few classes built-in to PHP which returned null upon failure were changed to throw an exception instead, for consistency[[50]](https://en.wikipedia.org/wiki/PHP#cite_note-50)
* Several unmaintained or deprecated [server application programming interfaces](https://en.wikipedia.org/wiki/Server_application_programming_interface) (SAPIs) and extensions were removed from the PHP core, most notably the legacy *mysql* extension[[51]](https://en.wikipedia.org/wiki/PHP#cite_note-51)
* The behavior of the *list()* operator was changed to remove support for strings[[52]](https://en.wikipedia.org/wiki/PHP#cite_note-52)
* Support for legacy ASP-style PHP code delimiters (*<%* and *%>*, *<script language=php>* and *</script>*) was removed[[53]](https://en.wikipedia.org/wiki/PHP#cite_note-53)
* An oversight allowing a [switch statement](https://en.wikipedia.org/wiki/Switch_statement) to have multiple *default* clauses was fixed[[54]](https://en.wikipedia.org/wiki/PHP#cite_note-54)
* Support for hexadecimal number support in some implicit conversions from strings to number types was removed[[55]](https://en.wikipedia.org/wiki/PHP#cite_note-55)
* The [left-shift](https://en.wikipedia.org/wiki/Left-shift_operator) and [right-shift](https://en.wikipedia.org/wiki/Right-shift_operator) operators were changed to behave more consistently across platforms[[56]](https://en.wikipedia.org/wiki/PHP#cite_note-integer_semantics-56)
* Conversions between integers and floating point numbers were tightened and implemented more consistently across platforms[[56]](https://en.wikipedia.org/wiki/PHP#cite_note-integer_semantics-56)[[57]](https://en.wikipedia.org/wiki/PHP#cite_note-57)

PHP 7 also included new language features. Most notably, it introduces return type declarations for functions,[[58]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-return-types-58) which complement the existing parameter type declarations, and support for the scalar types (integer, float, string, and boolean) in parameter and return type declarations.

PHP is a general-purpose scripting language that is especially suited to [server-side](https://en.wikipedia.org/wiki/Server-side_scripting) [web development](https://en.wikipedia.org/wiki/Web_development), in which case PHP generally runs on a [web server](https://en.wikipedia.org/wiki/Web_server). Any PHP code in a requested file is [executed](https://en.wikipedia.org/wiki/Execution_%28computing%29) by the PHP runtime, usually to create [dynamic web page](https://en.wikipedia.org/wiki/Dynamic_web_page) content or dynamic images used on websites or elsewhere.[[150]](https://en.wikipedia.org/wiki/PHP#cite_note-150) It can also be used for [command-line](https://en.wikipedia.org/wiki/Command-line) scripting and [client-side](https://en.wikipedia.org/wiki/Client-side) [graphical user interface](https://en.wikipedia.org/wiki/Graphical_user_interface) (GUI) applications. PHP can be deployed on most web servers, many [operating systems](https://en.wikipedia.org/wiki/Operating_system) and [platforms](https://en.wikipedia.org/wiki/Computing_platform), and can be used with many [relational database management systems](https://en.wikipedia.org/wiki/Relational_database_management_system) (RDBMS). Most [web hosting](https://en.wikipedia.org/wiki/Web_hosting) providers support PHP for use by their clients. It is available free of charge, and the PHP Group provides the complete source code for users to build, customize and extend for their own use.[[7]](https://en.wikipedia.org/wiki/PHP#cite_note-foundations-7)

[](https://en.wikipedia.org/wiki/File:Scheme_dynamic_page_en.svg)

Dynamic web page: example of [server-side scripting](https://en.wikipedia.org/wiki/Server-side_scripting) (PHP and MySQL).

PHP acts primarily as a [filter](https://en.wikipedia.org/wiki/Filter_%28software%29),[[151]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-151) taking input from a file or stream containing text and/or PHP instructions and outputting another stream of data. Most commonly the output will be HTML, although it could be [JSON](https://en.wikipedia.org/wiki/JSON), [XML](https://en.wikipedia.org/wiki/XML) or [binary data](https://en.wikipedia.org/wiki/Binary_data) such as image or audio formats. Since PHP 4, the PHP [parser](https://en.wikipedia.org/wiki/Parser) [compiles](https://en.wikipedia.org/wiki/Compiler) input to produce [bytecode](https://en.wikipedia.org/wiki/Bytecode) for processing by the [Zend Engine](https://en.wikipedia.org/wiki/Zend_Engine), giving improved performance over its [interpreter](https://en.wikipedia.org/wiki/Interpreter_%28computing%29) predecessor.[[152]](https://en.wikipedia.org/wiki/PHP#cite_note-152)

Originally designed to create dynamic [web pages](https://en.wikipedia.org/wiki/Web_page), PHP now focuses mainly on [server-side scripting](https://en.wikipedia.org/wiki/Server-side_scripting),[[153]](https://en.wikipedia.org/wiki/PHP#cite_note-153) and it is similar to other server-side scripting languages that provide dynamic content from a web server to a [client](https://en.wikipedia.org/wiki/Client_%28computing%29), such as [Microsoft](https://en.wikipedia.org/wiki/Microsoft)'s [ASP.NET](https://en.wikipedia.org/wiki/ASP.NET), [Sun Microsystems](https://en.wikipedia.org/wiki/Sun_Microsystems)' [JavaServer Pages](https://en.wikipedia.org/wiki/JavaServer_Pages),[[154]](https://en.wikipedia.org/wiki/PHP#cite_note-154) and [mod\_perl](https://en.wikipedia.org/wiki/Mod_perl). PHP has also attracted the development of many [software frameworks](https://en.wikipedia.org/wiki/Software_framework) that provide building blocks and a design structure to promote [rapid application development](https://en.wikipedia.org/wiki/Rapid_application_development) (RAD). Some of these include [PRADO](https://en.wikipedia.org/wiki/PRADO_%28framework%29), [CakePHP](https://en.wikipedia.org/wiki/CakePHP), [Symfony](https://en.wikipedia.org/wiki/Symfony), [CodeIgniter](https://en.wikipedia.org/wiki/CodeIgniter), [Laravel](https://en.wikipedia.org/wiki/Laravel), [Yii Framework](https://en.wikipedia.org/wiki/Yii_Framework), [Phalcon](https://en.wikipedia.org/wiki/Phalcon_%28framework%29) and [Zend Framework](https://en.wikipedia.org/wiki/Zend_Framework), offering features similar to other [web frameworks](https://en.wikipedia.org/wiki/Web_framework).

The [LAMP architecture](https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29) has become popular in the web industry as a way of deploying web applications.[[155]](https://en.wikipedia.org/wiki/PHP#cite_note-155) PHP is commonly used as the *P* in this bundle alongside [Linux](https://en.wikipedia.org/wiki/Linux), [Apache](https://en.wikipedia.org/wiki/Apache_HTTP_Server) and [MySQL](https://en.wikipedia.org/wiki/MySQL), although the *P* may also refer to [Python](https://en.wikipedia.org/wiki/Python_%28programming_language%29), [Perl](https://en.wikipedia.org/wiki/Perl), or some mix of the three. Similar packages, [WAMP](https://en.wikipedia.org/wiki/WAMP_%28software_bundle%29) and [MAMP](https://en.wikipedia.org/wiki/MAMP), are also available for [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) and [OS X](https://en.wikipedia.org/wiki/OS_X), with the first letter standing for the respective operating system. Although both PHP and Apache are provided as part of the Mac OS X base install, users of these packages seek a simpler installation mechanism that can be more easily kept up to date.

As of April 2007, over 20 million Internet domains had web services hosted on servers with PHP installed and mod\_php was recorded as the most popular [Apache HTTP Server](https://en.wikipedia.org/wiki/Apache_HTTP_Server) module.[[156]](https://en.wikipedia.org/wiki/PHP#cite_note-usage-156) As of October 2010, PHP was used as the server-side programming language on 75% of all websites whose server-side programming language was known[[157]](https://en.wikipedia.org/wiki/PHP#cite_note-W3Techs_usage_statistics_2010-10-29-157) (as of February 2014, the percentage had reached 82%[[158]](https://en.wikipedia.org/wiki/PHP#cite_note-W3Techs_usage_statistics_20140319-158)), and PHP was the most-used open source software within enterprises.[[159]](https://en.wikipedia.org/wiki/PHP#cite_note-159) [Web content management systems](https://en.wikipedia.org/wiki/Web_content_management_system) written in PHP include [MediaWiki](https://en.wikipedia.org/wiki/MediaWiki),[[160]](https://en.wikipedia.org/wiki/PHP#cite_note-160) [Joomla](https://en.wikipedia.org/wiki/Joomla),[[161]](https://en.wikipedia.org/wiki/PHP#cite_note-161) [eZ Publish](https://en.wikipedia.org/wiki/EZ_Publish), [SilverStripe](https://en.wikipedia.org/wiki/SilverStripe),[[162]](https://en.wikipedia.org/wiki/PHP#cite_note-162) [WordPress](https://en.wikipedia.org/wiki/WordPress),[[163]](https://en.wikipedia.org/wiki/PHP#cite_note-163) [Drupal](https://en.wikipedia.org/wiki/Drupal),[[164]](https://en.wikipedia.org/wiki/PHP#cite_note-164) [Moodle](https://en.wikipedia.org/wiki/Moodle),[[165]](https://en.wikipedia.org/wiki/PHP#cite_note-165) the user-facing portion of [Facebook](https://en.wikipedia.org/wiki/Facebook),[[166]](https://en.wikipedia.org/wiki/PHP#cite_note-166) and [Digg](https://en.wikipedia.org/wiki/Digg).[[167]](https://en.wikipedia.org/wiki/PHP#cite_note-167)

For specific and more advanced usage scenarios, PHP offers a well defined and documented way for writing custom extensions in [C](https://en.wikipedia.org/wiki/C_%28programming_language%29) or [C++](https://en.wikipedia.org/wiki/C%2B%2B).[[168]](https://en.wikipedia.org/wiki/PHP#cite_note-168)[[169]](https://en.wikipedia.org/wiki/PHP#cite_note-169)[[170]](https://en.wikipedia.org/wiki/PHP#cite_note-170)[[171]](https://en.wikipedia.org/wiki/PHP#cite_note-171)[[172]](https://en.wikipedia.org/wiki/PHP#cite_note-172)[[173]](https://en.wikipedia.org/wiki/PHP#cite_note-173)[[174]](https://en.wikipedia.org/wiki/PHP#cite_note-174) Besides extending the language itself in form of additional [libraries](https://en.wikipedia.org/wiki/Library_%28computing%29), extensions are providing a way for improving execution speed where it is critical and there is room for improvements by using a true [compiled language](https://en.wikipedia.org/wiki/Compiled_language).[[175]](https://en.wikipedia.org/wiki/PHP#cite_note-175)[[176]](https://en.wikipedia.org/wiki/PHP#cite_note-176) PHP also offers well defined ways for embedding itself into other software projects. That way PHP can be easily used as an internal [scripting language](https://en.wikipedia.org/wiki/Scripting_language) for another project, also providing tight interfacing with the project's specific internal [data structures](https://en.wikipedia.org/wiki/Data_structure).[[177]](https://en.wikipedia.org/wiki/PHP#cite_note-177)

PHP received mixed reviews due to lacking support for [multithreading](https://en.wikipedia.org/wiki/Multithreading_%28software%29) at the core language level,[[178]](https://en.wikipedia.org/wiki/PHP#cite_note-178) though using threads is made possible by the "pthreads" [PECL](https://en.wikipedia.org/wiki/PHP_Extension_Community_Library) extension.[[179]](https://en.wikipedia.org/wiki/PHP#cite_note-179)[[180]](https://en.wikipedia.org/wiki/PHP#cite_note-180)

As of January 2013, PHP was used in more than 240 million [websites](https://en.wikipedia.org/wiki/Website) (39% of those sampled) and was installed on 2.1 million [web servers](https://en.wikipedia.org/wiki/Web_server).

## Security

In 2013, 9% of all vulnerabilities listed by the [National Vulnerability Database](https://en.wikipedia.org/wiki/National_Vulnerability_Database) were linked to PHP;[[182]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-CVE-182) historically, about 30% of all vulnerabilities listed since 1996 in this database are linked to PHP. Technical security flaws of the language itself or of its core libraries are not frequent (22 in 2009, about 1% of the total although PHP applies to about 20% of programs listed).[[183]](https://en.wikipedia.org/wiki/PHP#cite_note-PHP-related_vulnerabilities_on_the_National_Vulnerability_Database-183) Recognizing that programmers make mistakes, some languages include [taint checking](https://en.wikipedia.org/wiki/Taint_checking) to automatically detect the lack of [input validation](https://en.wikipedia.org/wiki/Data_validation) which induces many issues. Such a feature is being developed for PHP,[[184]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-184) but its inclusion into a release has been rejected several times in the past.[[185]](https://en.wikipedia.org/wiki/PHP#cite_note-185)[[186]](https://en.wikipedia.org/wiki/PHP#cite_note-186)

There are advanced protection patches such as [Suhosin](https://en.wikipedia.org/wiki/Suhosin) and [Hardening](https://en.wikipedia.org/wiki/Hardening_%28computing%29)-Patch, especially designed for web hosting environments.[[187]](https://en.wikipedia.org/wiki/PHP#cite_note-187)

There are certain language features and configuration parameters (primarily the default values for such runtime settings) that make PHP applications prone to security issues. Among these, [magic\_quotes\_gpc](https://en.wikipedia.org/wiki/Magic_quotes) and register\_globals[[188]](https://en.wikipedia.org/wiki/PHP" \l "cite_note-register-globals-188) configuration directives are the best known; the latter made any URL parameters become PHP variables, opening a path for serious security vulnerabilities by allowing an attacker to set the value of any uninitialized global variable and interfere with the execution of a PHP script. Support for "[magic quotes](https://en.wikipedia.org/wiki/Magic_quotes)" and "register globals" has been deprecated as of PHP 5.3.0, and removed as of PHP 5.4.0.[[189]](https://en.wikipedia.org/wiki/PHP#cite_note-magic-quotes-189)

Another example for the runtime settings vulnerability comes from failing to disable PHP execution (via engine configuration directive)[[190]](https://en.wikipedia.org/wiki/PHP#cite_note-190) for the directory where uploaded images are stored; leaving the default settings can result in execution of malicious PHP code embedded within the uploaded images.[[191]](https://en.wikipedia.org/wiki/PHP#cite_note-191)[[192]](https://en.wikipedia.org/wiki/PHP#cite_note-192)[[193]](https://en.wikipedia.org/wiki/PHP#cite_note-193) Also, leaving enabled the dynamic loading of PHP extensions (via enable\_dl configuration directive)[[194]](https://en.wikipedia.org/wiki/PHP#cite_note-194) in a [shared web hosting](https://en.wikipedia.org/wiki/Shared_web_hosting) environment can lead to security issues.[[195]](https://en.wikipedia.org/wiki/PHP#cite_note-195)[[196]](https://en.wikipedia.org/wiki/PHP#cite_note-196)

Also, implied [type conversions](https://en.wikipedia.org/wiki/Type_conversion) that result in incompatible values being treated as identical against the programmer's intent can lead to security issues. For example, the result of the comparison *0e1234 == 0* comparison is *true* because the first compared value is treated as [scientific notation](https://en.wikipedia.org/wiki/Scientific_notation) having the value (0×101234), i.e. *zero*. This feature resulted in authentication vulnerabilities in [Simple Machines Forum](https://en.wikipedia.org/wiki/Simple_Machines_Forum),[[197]](https://en.wikipedia.org/wiki/PHP#cite_note-197) [Typo3](https://en.wikipedia.org/wiki/Typo3)[[198]](https://en.wikipedia.org/wiki/PHP#cite_note-198) and [phpBB](https://en.wikipedia.org/wiki/PhpBB)[[199]](https://en.wikipedia.org/wiki/PHP#cite_note-199) when [MD5](https://en.wikipedia.org/wiki/MD5) [password hashes](https://en.wikipedia.org/wiki/Password_hashing) were compared. Instead, either the function [strcmp](https://en.wikipedia.org/wiki/Strcmp) or the identity operator (*===*) should be used; *0e1234 === 0* results in *false*.[[200]](https://en.wikipedia.org/wiki/PHP#cite_note-200)

In a 2013 analysis of over 170,000 [website defacements](https://en.wikipedia.org/wiki/Website_defacement), published by [Zone-H](https://en.wikipedia.org/wiki/Zone-H), the most frequently (53%) used technique was exploitation of [file inclusion vulnerability](https://en.wikipedia.org/wiki/File_inclusion_vulnerability), mostly related to insecure usage of the PHP functions *include*, *require*, and *allow\_url\_fopen*.

**MySQL**

**MySQL** (officially pronounced as [/maɪ ˌɛskjuːˈɛl/](https://en.wikipedia.org/wiki/Help:IPA_for_English) "My S-Q-L",[[5]](https://en.wikipedia.org/wiki/MySQL#cite_note-whatismysql-5)) is an [open-source](https://en.wikipedia.org/wiki/Open-source) [relational database management system](https://en.wikipedia.org/wiki/Relational_database_management_system) (RDBMS);[[6]](https://en.wikipedia.org/wiki/MySQL#cite_note-6) in July 2013, it was the world's second most[[a]](https://en.wikipedia.org/wiki/MySQL#cite_note-9) widely used RDBMS, and the most widely used open-source [client–server model](https://en.wikipedia.org/wiki/Client%E2%80%93server_model) RDBMS.[[9]](https://en.wikipedia.org/wiki/MySQL#cite_note-10) It is named after co-founder [Michael Widenius](https://en.wikipedia.org/wiki/Michael_Widenius)'s daughter, My.[[10]](https://en.wikipedia.org/wiki/MySQL#cite_note-11) The [SQL](https://en.wikipedia.org/wiki/SQL) acronym stands for [Structured Query Language](https://en.wikipedia.org/wiki/Structured_Query_Language). The MySQL development project has made its [source code](https://en.wikipedia.org/wiki/Source_code) available under the terms of the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License), as well as under a variety of [proprietary](https://en.wikipedia.org/wiki/Proprietary_software) agreements. MySQL was owned and sponsored by a single [for-profit](https://en.wikipedia.org/wiki/Business) firm, the [Swedish](https://en.wikipedia.org/wiki/Sweden) company [MySQL AB](https://en.wikipedia.org/wiki/MySQL_AB), now owned by [Oracle Corporation](https://en.wikipedia.org/wiki/Oracle_Corporation).[[11]](https://en.wikipedia.org/wiki/MySQL#cite_note-sunacquire-12) For proprietary use, several paid editions are available, and offer additional functionality.

MySQL is a popular choice of database for use in web applications, and is a central component of the widely used [LAMP](https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29) open-source web application software stack (and other "[AMP](https://en.wikipedia.org/wiki/List_of_AMP_packages)" stacks). LAMP is an acronym for "[Linux](https://en.wikipedia.org/wiki/Linux), [Apache](https://en.wikipedia.org/wiki/Apache_HTTP_Server), MySQL, [Perl](https://en.wikipedia.org/wiki/Perl)/[PHP](https://en.wikipedia.org/wiki/PHP)/[Python](https://en.wikipedia.org/wiki/Python_%28programming_language%29)". [Free-software](https://en.wikipedia.org/wiki/Free_software) open-source projects that require a full-featured database management system often use MySQL. Applications that use the MySQL database include: [TYPO3](https://en.wikipedia.org/wiki/TYPO3), [MODx](https://en.wikipedia.org/wiki/MODx), [Joomla](https://en.wikipedia.org/wiki/Joomla), [WordPress](https://en.wikipedia.org/wiki/WordPress), [phpBB](https://en.wikipedia.org/wiki/PhpBB), [MyBB](https://en.wikipedia.org/wiki/MyBB), [Drupal](https://en.wikipedia.org/wiki/Drupal) and other software. MySQL is also used in many high-profile, large-scale [websites](https://en.wikipedia.org/wiki/Website), including [Google](https://en.wikipedia.org/wiki/Google)[[12]](https://en.wikipedia.org/wiki/MySQL#cite_note-mysqlatgoogle-13)[[13]](https://en.wikipedia.org/wiki/MySQL#cite_note-14) (though not for searches), [Facebook](https://en.wikipedia.org/wiki/Facebook),[[14]](https://en.wikipedia.org/wiki/MySQL#cite_note-mysqlatfacebook-15)[[15]](https://en.wikipedia.org/wiki/MySQL#cite_note-16)[[16]](https://en.wikipedia.org/wiki/MySQL#cite_note-17) [Twitter](https://en.wikipedia.org/wiki/Twitter),[[17]](https://en.wikipedia.org/wiki/MySQL#cite_note-18) [Flickr](https://en.wikipedia.org/wiki/Flickr),[[18]](https://en.wikipedia.org/wiki/MySQL#cite_note-19) and [YouTube](https://en.wikipedia.org/wiki/YouTube).[[19]](https://en.wikipedia.org/wiki/MySQL#cite_note-20)

On all platforms except Windows, MySQL ships with no [GUI](https://en.wikipedia.org/wiki/Graphical_user_interface) tools to administer MySQL databases or manage data contained within the databases. Users may use the included [command line](https://en.wikipedia.org/wiki/Command_line) tools,[[20]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-mysql_.E2.80.94_The_MySQL_Command-Line_Tool-21)[[21]](https://en.wikipedia.org/wiki/MySQL#cite_note-mysqladmin_-_the_MySQL_command-line_tool-22) or install [MySQL Workbench](http://dev.mysql.com/downloads/workbench/) via a separate download. Many third party GUI tools are also available

### Milestones

Notable milestones in MySQL development include:

* Original development of MySQL by [Michael Widenius](https://en.wikipedia.org/wiki/Michael_Widenius) and [David Axmark](https://en.wikipedia.org/wiki/David_Axmark) beginning in 1994[[31]](https://en.wikipedia.org/wiki/MySQL#cite_note-32)
* First internal release on 23 May 1995
* Version 3.19: End of 1996, from www.tcx.se
* Version 3.20: January 1997
* Windows version was released on 8 January 1998 for Windows 95 and NT
* Version 3.21: production release 1998, from www.mysql.com
* Version 3.22: alpha, beta from 1998
* Version 3.23: beta from June 2000, production release 22 January 2001[[32]](https://en.wikipedia.org/wiki/MySQL#cite_note-33)
* Version 4.0: beta from August 2002, production release March 2003 ([unions](https://en.wikipedia.org/wiki/Set_operations_%28SQL%29))
* Version 4.01: beta from August 2003, Jyoti[[*clarification needed*](https://en.wikipedia.org/wiki/Wikipedia:Please_clarify)][[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)] adopts MySQL for database tracking
* Version 4.1: beta from June 2004, production release October 2004 ([R-trees](https://en.wikipedia.org/wiki/R-tree) and [B-trees](https://en.wikipedia.org/wiki/B-tree), subqueries, prepared statements)
* Version 5.0: beta from March 2005, production release October 2005 (cursors, stored procedures, triggers, views, [XA transactions](https://en.wikipedia.org/wiki/Database_transaction))

The developer of the Federated Storage Engine states that "The Federated Storage Engine is a [proof-of-concept](https://en.wikipedia.org/wiki/Proof_of_concept) storage engine",[[33]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-34) but the main distributions of MySQL version 5.0 included it and turned it on by default. Documentation of some of the short-comings appears in "MySQL Federated Tables: The Missing Manual".[[34]](https://en.wikipedia.org/wiki/MySQL#cite_note-35)

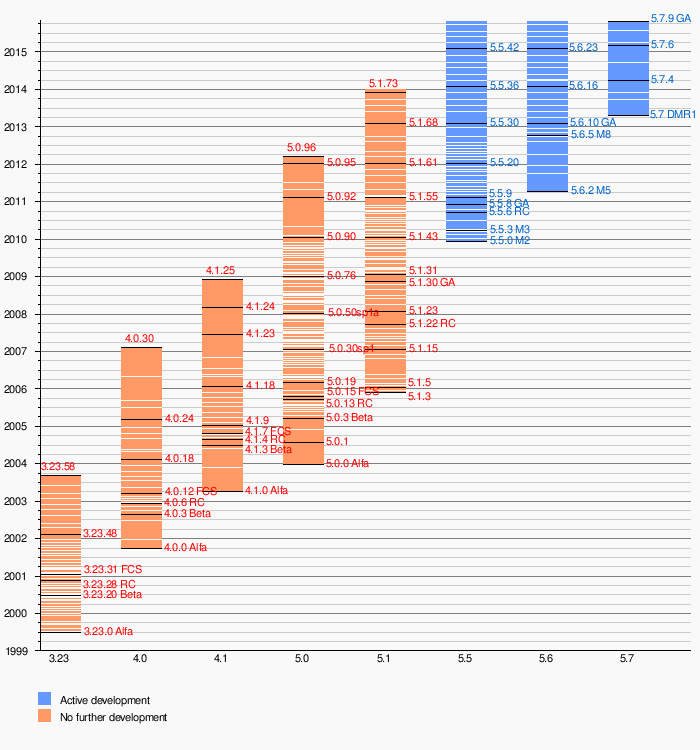
* [Sun Microsystems](https://en.wikipedia.org/wiki/Sun_Microsystems) acquired [MySQL AB](https://en.wikipedia.org/wiki/MySQL_AB) in 2008.[[35]](https://en.wikipedia.org/wiki/MySQL#cite_note-36)
* Version 5.1: production release 27 November 2008 (event scheduler, [partitioning](https://en.wikipedia.org/wiki/Partition_%28database%29), plugin API, row-based replication, [server log](https://en.wikipedia.org/wiki/Server_log) tables)

Version 5.1 contained 20 known crashing and wrong result bugs in addition to the 35 present in version 5.0 *(almost all fixed as of release 5.1.51)*.[[36]](https://en.wikipedia.org/wiki/MySQL#cite_note-37)

MySQL 5.1 and 6.0-alpha showed poor performance when used for [data warehousing](https://en.wikipedia.org/wiki/Data_warehousing) – partly due to its inability to utilize multiple CPU cores for processing a single query.[[37]](https://en.wikipedia.org/wiki/MySQL#cite_note-38)

* Oracle acquired Sun Microsystems on 27 January 2010.[[38]](https://en.wikipedia.org/wiki/MySQL#cite_note-39)[[39]](https://en.wikipedia.org/wiki/MySQL#cite_note-40)[[40]](https://en.wikipedia.org/wiki/MySQL#cite_note-41)
* The day Oracle announced the purchase of Sun, Michael "Monty" Widenius forked MySQL, launching [MariaDB](https://en.wikipedia.org/wiki/MariaDB), and took a swath of MySQL developers with him.[[41]](https://en.wikipedia.org/wiki/MySQL#cite_note-dead-42)
* MySQL Server 5.5 was generally available (as of December 2010). Enhancements and features include:
  + The default storage engine is InnoDB, which supports transactions and referential integrity constraints.
  + Improved InnoDB I/O subsystem[[42]](https://en.wikipedia.org/wiki/MySQL#cite_note-43)
  + Improved [SMP](https://en.wikipedia.org/wiki/Symmetric_multiprocessing) support[[43]](https://en.wikipedia.org/wiki/MySQL#cite_note-44)
  + Semisynchronous replication.
  + SIGNAL and RESIGNAL statement in compliance with the SQL standard.
  + Support for supplementary Unicode character sets utf16, utf32, and utf8mb4.
  + New options for user-defined partitioning.
* MySQL Server 6.0.11-alpha was announced[[44]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-45) on 22 May 2009 as the last release of the 6.0 line. Future MySQL Server development uses a New Release Model. Features developed for 6.0 are being incorporated into future releases.
* The general availability of MySQL 5.6 was announced in February 2013. New features included performance improvements to the [query optimizer](https://en.wikipedia.org/wiki/Query_optimizer), higher transactional throughput in InnoDB, new [NoSQL](https://en.wikipedia.org/wiki/NoSQL_%28concept%29)-style memcached APIs, improvements to partitioning for querying and managing very large tables, TIMESTAMP column type that correctly stores milliseconds, improvements to replication, and better performance monitoring by expanding the data available through the PERFORMANCE\_SCHEMA.[[45]](https://en.wikipedia.org/wiki/MySQL#cite_note-46) The InnoDB storage engine also included support for full-text search and improved group commit performance.
* The general availability of MySQL 5.7 was announced in October 2015

**Version History**



## Features

MySQL is offered under two different editions: the open source MySQL Community Server and the proprietary [Enterprise Server](https://en.wikipedia.org/wiki/MySQL_Enterprise).[[72]](https://en.wikipedia.org/wiki/MySQL#cite_note-73) MySQL Enterprise Server is differentiated by a series of proprietary extensions which install as server plugins, but otherwise shares the version numbering system and is built from the same code base.

Major features as available in MySQL 5.6:

* A broad subset of [ANSI SQL 99](https://en.wikipedia.org/wiki/SQL:1999), as well as extensions
* Cross-platform support
* [Stored procedures](https://en.wikipedia.org/wiki/Stored_procedure), using a procedural language that closely adheres to [SQL/PSM](https://en.wikipedia.org/wiki/SQL/PSM)[[73]](https://en.wikipedia.org/wiki/MySQL#cite_note-HarrisonFeuerstein2008-74)
* [Triggers](https://en.wikipedia.org/wiki/Database_trigger)
* [Cursors](https://en.wikipedia.org/wiki/Cursor_%28databases%29)
* Updatable [views](https://en.wikipedia.org/wiki/View_%28SQL%29)
* [Online DDL](https://en.wikipedia.org/wiki/Data_Definition_Language) when using the InnoDB Storage Engine.
* [Information schema](https://en.wikipedia.org/wiki/Information_schema)
* Performance Schema that collects and aggregates statistics about server execution and query performance for monitoring purposes.[[74]](https://en.wikipedia.org/wiki/MySQL#cite_note-75)
* A set of SQL Mode options to control runtime behavior, including a strict mode to better adhere to SQL standards.
* [X/Open XA](https://en.wikipedia.org/wiki/X/Open_XA) [distributed transaction processing](https://en.wikipedia.org/wiki/Distributed_transaction_processing) (DTP) support; [two phase commit](https://en.wikipedia.org/wiki/Two-phase-commit_protocol) as part of this, using the default [InnoDB](https://en.wikipedia.org/wiki/InnoDB) storage engine
* Transactions with [savepoints](https://en.wikipedia.org/wiki/Savepoint) when using the default InnoDB Storage Engine. The NDB Cluster Storage Engine also supports transactions.
* [ACID](https://en.wikipedia.org/wiki/Atomicity,_consistency,_isolation,_durability) compliance when using InnoDB and NDB Cluster Storage Engines[[75]](https://en.wikipedia.org/wiki/MySQL#cite_note-76)
* [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer) support
* Query [caching](https://en.wikipedia.org/wiki/Cache_%28computing%29)
* Sub-[SELECTs](https://en.wikipedia.org/wiki/Select_%28SQL%29) (i.e. nested SELECTs)
* Built-in [Replication](https://en.wikipedia.org/wiki/Database_replication) support (i.e. Master-Master Replication & Master-Slave Replication) with one master per slave, many slaves per master.[[76]](https://en.wikipedia.org/wiki/MySQL#cite_note-77) [Multi-master replication](https://en.wikipedia.org/wiki/Multi-master_replication) is provided in [MySQL Cluster](https://en.wikipedia.org/wiki/MySQL_Cluster),[[77]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-78) and multi-master support can be added to unclustered configurations using Galera Cluster.[[78]](https://en.wikipedia.org/wiki/MySQL#cite_note-79)
* Full-text [indexing](https://en.wikipedia.org/wiki/Index_%28database%29) and searching[[b]](https://en.wikipedia.org/wiki/MySQL#cite_note-80)
* Embedded database library
* [Unicode](https://en.wikipedia.org/wiki/Unicode) support[[c]](https://en.wikipedia.org/wiki/MySQL#cite_note-81)
* Partitioned tables with pruning of partitions in optimizer
* [Shared-nothing](https://en.wikipedia.org/wiki/Shared-nothing) clustering through [MySQL Cluster](https://en.wikipedia.org/wiki/MySQL_Cluster)
* Multiple storage engines, allowing one to choose the one that is most effective for each table in the application.[[d]](https://en.wikipedia.org/wiki/MySQL#cite_note-82)
* Native storage engines [InnoDB](https://en.wikipedia.org/wiki/InnoDB), [MyISAM](https://en.wikipedia.org/wiki/MyISAM), Merge, Memory (heap), [Federated](https://en.wikipedia.org/wiki/MySQL_Federated), Archive, [CSV](https://en.wikipedia.org/wiki/Comma-separated_values), Blackhole, NDB Cluster.
* Commit grouping, gathering multiple transactions from multiple connections together to increase the number of commits per second.

The developers release minor updates of the MySQL Server approximately every two months. The sources can be obtained from MySQL's website or from MySQL's [GitHub](https://en.wikipedia.org/wiki/Git_%28software%29) repository, both under the GPL license.

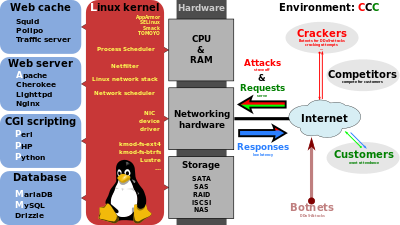
### Limitations

Like other SQL databases, MySQL does not comply with the full [SQL](https://en.wikipedia.org/wiki/SQL) standard for some of the implemented functionality, including foreign key references when using some storage engines other than the default of InnoDB,[[79]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-83) and check constraints.[[80]](https://en.wikipedia.org/wiki/MySQL#cite_note-84)

Up until MySQL 5.7, triggers are limited to one per action / timing, meaning that at most one trigger can be defined to be executed after an INSERT operation, and one before INSERT on the same table.[[81]](https://en.wikipedia.org/wiki/MySQL#cite_note-dev.mysql.com-85) No triggers can be defined on views.[[81]](https://en.wikipedia.org/wiki/MySQL#cite_note-dev.mysql.com-85)

MySQL database's inbuilt functions like UNIX\_TIMESTAMP() will return 0 after 03:14:07 [UTC](https://en.wikipedia.org/wiki/UTC) on [19 January 2038](https://en.wikipedia.org/wiki/Year_2038_problem).[[82]](https://en.wikipedia.org/wiki/MySQL#cite_note-86)

### Deployment

[](https://en.wikipedia.org/wiki/File:LAMP_software_bundle.svg)

[LAMP](https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29) software bundle, displayed here together with [Squid](https://en.wikipedia.org/wiki/Squid_%28software%29).

MySQL can be built and installed manually from source code, but it is more commonly installed from a binary package unless special customizations are required. On most [Linux distributions](https://en.wikipedia.org/wiki/Linux_distribution), the [package management system](https://en.wikipedia.org/wiki/Package_management_system) can download and install MySQL with minimal effort, though further configuration is often required to adjust security and optimization settings.

Though MySQL began as a low-end alternative to more powerful proprietary databases, it has gradually evolved to support higher-scale needs as well. It is still most commonly used in small to medium scale single-server deployments, either as a component in a [LAMP](https://en.wikipedia.org/wiki/LAMP_%28software_bundle%29)-based web application or as a standalone database server. Much of MySQL's appeal originates in its relative simplicity and ease of use, which is enabled by an ecosystem of open source tools such as [phpMyAdmin](https://en.wikipedia.org/wiki/PhpMyAdmin). In the medium range, MySQL can be scaled by deploying it on more powerful hardware, such as a multi-processor server with gigabytes of memory.

There are however limits to how far performance can scale on a single server ('scaling up'), so on larger scales, multi-server MySQL ('scaling out') deployments are required to provide improved performance and reliability. A typical high-end configuration can include a powerful master database which handles data write operations and is [replicated](https://en.wikipedia.org/wiki/Database_replication) to multiple slaves that handle all read operations.[[83]](https://en.wikipedia.org/wiki/MySQL#cite_note-87) The master server continually pushes binlog events to connected slaves so in the event of failure a slave can be promoted to become the new master, minimizing downtime. Further improvements in performance can be achieved by caching the results from database queries in memory using [memcached](https://en.wikipedia.org/wiki/Memcached), or breaking down a database into smaller chunks called [shards](https://en.wikipedia.org/wiki/Shard_%28database_architecture%29) which can be spread across a number of distributed server clusters.

### Backup software

Backup software are computer programs used to perform backup; they create supplementary exact copies of files, databases or entire computers. These programs may later use the supplementary copies to restore the original contents in the event of data loss.

[Filesystem snapshot](https://en.wikipedia.org/wiki/Filesystem_snapshot) or [volume manager snapshot](https://en.wikipedia.org/wiki/Volume_manager_snapshot) backups are performed by using an external tool provided by the operating system (such as [Logical Volume Manager](https://en.wikipedia.org/wiki/Logical_Volume_Manager_%28Linux%29) in Linux) or storage device, with additional support from MySQL for ensuring consistency of such snapshots.

mysqldump is a logical backup tool included with both community and enterprise editions of MySQL. It supports backing up from all storage engines. MySQL Enterprise Backup is a hot backup utility included as part of the MySQL Enterprise subscription from Oracle, offering native InnoDB hot backup, as well as backup for other storage engines. XtraBackup is an open-source MySQL hot backup software program. Some notable features include hot, non-locking backups for InnoDB storage, incremental backups, streaming, parallel-compressed backups, throttling based on the number of I/O operations per second, etc.[[85]](https://en.wikipedia.org/wiki/MySQL#cite_note-89)

### High availability

Ensuring [high availability](https://en.wikipedia.org/wiki/High_availability) requires a certain amount of redundancy in the system. For database systems, the redundancy traditionally takes the form of having a primary server acting as a master, and using [replication](https://en.wikipedia.org/wiki/Replication_%28computing%29) to keep secondaries available to take over in case the primary fails. This means that the "server" that the application connects to is in reality a collection of servers, not a single server. In a similar manner, if the application is using a [sharded](https://en.wikipedia.org/wiki/Shard_%28database_architecture%29) database, it is in reality working with a collection of servers, not a single server. In this case, a collection of servers is usually referred to as a *farm.*[[86]](https://en.wikipedia.org/wiki/MySQL#cite_note-fabric-mats-90)

One of the projects aiming to provide high availability for MySQL is *MySQL Fabric*, an integrated system for managing a collection of MySQL servers, and a [framework](https://en.wikipedia.org/wiki/Software_framework) on top of which high availability and database sharding is built. MySQL Fabric is open-source and is intended to be extensible, easy to use, and to support procedure execution even in the presence of failure, providing an execution model usually called *resilient execution.* MySQL client libraries are extended so they are hiding the complexities of handling [failover](https://en.wikipedia.org/wiki/Failover) in the event of a server failure, as well as correctly dispatching transactions to the shards. As of September 2013, there is support for Fabric-aware versions of Connector/[J](https://en.wikipedia.org/wiki/J_Sharp), Connector/[PHP](https://en.wikipedia.org/wiki/PHP), Connector/[Python](https://en.wikipedia.org/wiki/Python_%28programming_language%29), as well as some rudimentary support for [Hibernate](https://en.wikipedia.org/wiki/Hibernate_%28Java%29) and [Doctrine](https://en.wikipedia.org/wiki/Doctrine_%28PHP%29). As of May 2014, MySQL Fabric is in the [general availability](https://en.wikipedia.org/wiki/General_availability) stage of development.[[87]](https://en.wikipedia.org/wiki/MySQL#cite_note-91)

### Cloud deployment

Main article: [Cloud database](https://en.wikipedia.org/wiki/Cloud_database)

MySQL can also be run on [cloud computing](https://en.wikipedia.org/wiki/Cloud_computing) platforms such as [Amazon EC2](https://en.wikipedia.org/wiki/Amazon_EC2). Some common deployment models for MySQL on the cloud are:

Virtual machine image

In this implementation, cloud users can upload a machine image of their own with MySQL installed, or use a ready-made machine image with an optimized installation of MySQL on it, such as the one provided by Amazon EC2.[[88]](https://en.wikipedia.org/wiki/MySQL#cite_note-92)

MySQL as a service

Some cloud platforms offer MySQL "as a service". In this configuration, application owners do not have to install and maintain the MySQL database on their own. Instead, the database service provider takes responsibility for installing and maintaining the database, and application owners pay according to their usage.[[89]](https://en.wikipedia.org/wiki/MySQL#cite_note-readwriteweb-93) Notable cloud-based MySQL services are the [Amazon Relational Database Service](https://en.wikipedia.org/wiki/Amazon_Relational_Database_Service); [Rackspace](https://en.wikipedia.org/wiki/Rackspace); [HP Converged Cloud](https://en.wikipedia.org/wiki/HP_Converged_Cloud); [Heroku](https://en.wikipedia.org/wiki/Heroku) and [Jelastic](https://en.wikipedia.org/wiki/Jelastic).

Managed MySQL cloud hosting

In this implementation, the database is not offered as a service, but the cloud provider hosts the database and manages it on the application owner's behalf. As of 2011, of the major cloud providers, only [Terremark](https://en.wikipedia.org/wiki/Terremark) and Rackspace offer managed hosting for MySQL databases

## User interfaces

### Graphical user interfaces

A [graphical user interface](https://en.wikipedia.org/wiki/Graphical_user_interface) (GUI) is a type of interface that allows users to interact with electronic devices or programs through graphical icons and visual indicators such as secondary notation, as opposed to text-based interfaces, typed command labels or text navigation. GUIs are easier to learn than command-line interfaces (CLIs),[4][5][6] which require commands to be typed on the keyboard.

Third-party proprietary and free graphical administration applications (or "front ends") are available that integrate with MySQL and enable users to work with database structure and data visually. Some well-known front ends are:

[](https://en.wikipedia.org/wiki/File:The_MySQL_Workbench_startup_screen.png)

[MySQL Workbench](https://en.wikipedia.org/wiki/MySQL_Workbench) running on OS X

MySQL Workbench

[MySQL Workbench](https://en.wikipedia.org/wiki/MySQL_Workbench) is the official integrated environment for MySQL. It was developed by MySQL AB, and enables users to graphically administer MySQL databases and visually design database structures. MySQL Workbench replaces the previous package of software, [MySQL GUI Tools](https://en.wikipedia.org/wiki/MySQL_GUI_Tools). Similar to other third-party packages, but still considered the authoritative MySQL front end, MySQL Workbench lets users manage database design & modeling, SQL development (replacing MySQL Query Browser) and Database administration (replacing MySQL Administrator).

MySQL Workbench is available in two editions, the regular [free and open source](https://en.wikipedia.org/wiki/Free_and_open_source_software) *Community Edition* which may be downloaded from the MySQL website, and the proprietary *Standard Edition* which extends and improves the feature set of the Community Edition.

Adminer

[Adminer](https://en.wikipedia.org/wiki/Adminer) (formerly known as phpMinAdmin) is a free MySQL front end for managing content in MySQL databases (since version 2, it also works on PostgreSQL, MS SQL, SQLite and Oracle SQL databases). Adminer is distributed under the Apache license (or GPL v2) in the form of a single PHP file (around 300 KiB in size), and is capable of managing multiple databases, with many CSS skins available. Its author is Jakub Vrána who started to develop this tool as a light-weight alternative to phpMyAdmin, in July 2007.

Database Workbench

[Database Workbench](https://en.wikipedia.org/wiki/Database_Workbench) is a software application for development and administration of multiple relational databases using SQL, with interoperationality between different database systems, developed by Upscene Productions.

Because Databases Workbench supports multiple database systems, it can provide software developers with the same interface and development environment for these otherwise different database systems and also includes cross database tools.

Database Workbench supports the following relational databases: Oracle Database, Microsoft SQL Server, SQL Anywhere, Firebird, NexusDB, InterBase, MySQL and MariaDB. Database Workbench 5 runs on 32-bit or 64 bit Windows platforms. Under Linux, FreeBSD or Mac OS X Database Workbench can operate using Wine.

DBEdit

[DBEdit](https://en.wikipedia.org/wiki/DBEdit) is a database editor, which can connect to an Oracle, DB2, MySQL and any database that provides a JDBC driver. It runs on Windows, Linux and Solaris. DBEdit is free and open source software and distributed under the GNU General Public License. The source code is hosted on SourceForge.

HeidiSQL

[HeidiSQL](https://en.wikipedia.org/wiki/HeidiSQL), previously known as MySQL-Front, is a free and open source client, or frontend for MySQL (and for its forks like MariaDB and Percona Server, Microsoft SQL Server and PostgreSQL). HeidiSQL is developed by German programmer Ansgar Becker and a few other contributors in Delphi. To manage databases with HeidiSQL, users must login to a local or remote MySQL server with acceptable credentials, creating a session. Within this session users may manage MySQL Databases within the connected MySQL server, disconnecting from the server when done. Its feature set is sufficient for most common and advanced database, table and data record operations but remains in active development to move towards the full functionality expected in a MySQL Frontend.

LibreOffice Base

[LibreOffice](https://en.wikipedia.org/wiki/LibreOffice) Base allows the creation and management of databases, preparation of forms and reports that provide end users easy access to data. Like [Microsoft Access](https://en.wikipedia.org/wiki/Microsoft_Access), it can be used as a front-end for various database systems, including Access databases (JET), ODBC data sources, and MySQL or [PostgreSQL](https://en.wikipedia.org/wiki/PostgreSQL)[[92]](https://en.wikipedia.org/wiki/MySQL#cite_note-96)

Navicat

[Navicat](https://en.wikipedia.org/wiki/Navicat) is a series of graphical database management and development software produced by PremiumSoft CyberTech Ltd. for MySQL, MariaDB, Oracle, SQLite, PostgreSQL and Microsoft SQL Server. It has an Explorer-like graphical user interface and supports multiple database connections for local and remote databases. Its design is made to meet the needs of a variety of audiences, from database administrators and programmers to various businesses/companies that serve clients and share information with partners.

Navicat is a cross-platform tool and works on Microsoft Windows, OS X and Linux platforms. Upon purchase, users are able to select a language for the software from eight available languages: English, French, German, Spanish, Japanese, Polish, Simplified Chinese and Traditional Chinese.

OpenOffice.org

[OpenOffice.org Base](https://en.wikipedia.org/wiki/OpenOffice.org_Base) is freely available and can manage MySQL databases if the entire suite is installed.

phpMyAdmin

[phpMyAdmin](https://en.wikipedia.org/wiki/PhpMyAdmin) is a free and open source tool written in PHP intended to handle the administration of MySQL with the use of a web browser. It can perform various tasks such as creating, modifying or deleting databases, tables, fields or rows; executing SQL statements; or managing users and permissions. The software, which is available in 78 languages,[[93]](https://en.wikipedia.org/wiki/MySQL" \l "cite_note-97) is maintained by *The phpMyAdmin Project*.[[94]](https://en.wikipedia.org/wiki/MySQL#cite_note-98)

It can import data from CSV and SQL, and transform stored data into any format using a set of predefined functions, like displaying BLOB-data as images or download-links.

SQLBuddy

[SQLBuddy](https://en.wikipedia.org/wiki/SQLBuddy) is an open source web based application written in PHP intended to handle the administration of MySQL and SQLite with the use of a Web browser. The project places an emphasis on ease of installation and a simple user interface.

SQLyog

[SQLyog](https://en.wikipedia.org/wiki/SQLyog) is a GUI tool available in free as well as paid versions. Data manipulations (e.g., insert, update, and delete) may be done from a spreadsheet-like interface. Its editor has syntax highlighting and various automatic formatting options. Both raw table data and a result set from a query can be manipulated. Its data search feature uses Google-like search syntax and translates to SQL transparently for the user. It has a backup tool for performing unattended backups. Backups may be compressed and optionally stored as a file-per-table as well as identified with a timestamp.

Toad for MySQL

[Toad for MySQL](https://en.wikipedia.org/wiki/TOAD_%28software%29) is a software application from Dell Software that database developers, database administrators and data analysts use to manage both relational and non-relational databases using SQL. Toad supports many databases and environments. It runs on all 32-bit/64-bit Windows platforms, including Microsoft Windows Server,Windows XP, Windows Vista,Windows 7 and 8 (32-Bit or 64-Bit). Dell Software has also released a Toad Mac Edition. Dell provides Toad in commercial and trial/freeware versions. The Freeware version is available from the ToadWorld.com community.

Webmin

[Webmin](https://en.wikipedia.org/wiki/Webmin) is a web-based system configuration tool for Unix-like systems, although recent versions can also be installed and run on Windows. With it, it is possible to configure operating system internals, such as users, disk quotas, services or configuration files, as well as modify and control open source apps, such as the Apache HTTP Server, PHP or MySQL.

Webmin is largely based on Perl, running as its own process and web server. It defaults to TCP port 10000 for communicating, and can be configured to use SSL if OpenSSL is installed with additional required Perl Modules.

It is built around modules, which have an interface to the configuration files and the Webmin server. This makes it easy to add new functionality. Due to Webmin's modular design, it is possible for anyone who is interested to write plugins for desktop configuration.

Webmin also allows for controlling many machines through a single interface, or seamless login on other webmin hosts on the same subnet or LAN.

AES

The **Advanced Encryption Standard** (**AES**), also known as **Rijndael**[[4]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-Rijndael-4)[[5]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-Rijndael-ammended.pdf-5) (its original name), is a specification for the [encryption](https://en.wikipedia.org/wiki/Encryption) of electronic data established by the U.S. [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST) in 2001.[[6]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-fips-197-6)

AES is based on the Rijndael [cipher](https://en.wikipedia.org/wiki/Cipher)[[5]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-Rijndael-ammended.pdf-5) developed by two [Belgian](https://en.wikipedia.org/wiki/Belgium) cryptographers, [Joan Daemen](https://en.wikipedia.org/wiki/Joan_Daemen) and [Vincent Rijmen](https://en.wikipedia.org/wiki/Vincent_Rijmen), who submitted a proposal to NIST during the AES selection process.[[7]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-7) Rijndael is a family of ciphers with different key and block sizes.

For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.

AES has been adopted by the [U.S. government](https://en.wikipedia.org/wiki/Federal_government_of_the_United_States) and is now used worldwide. It supersedes the [Data Encryption Standard](https://en.wikipedia.org/wiki/Data_Encryption_Standard) (DES),[[8]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-8) which was published in 1977. The algorithm described by AES is a [symmetric-key algorithm](https://en.wikipedia.org/wiki/Symmetric-key_algorithm), meaning the same key is used for both encrypting and decrypting the data.

In the United States, AES was announced by the NIST as U.S. [FIPS](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard) PUB 197 (FIPS 197) on November 26, 2001.[[6]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-fips-197-6) This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable (see [Advanced Encryption Standard process](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard_process) for more details).

AES became effective as a federal government standard on May 26, 2002 after approval by the [Secretary of Commerce](https://en.wikipedia.org/wiki/United_States_Secretary_of_Commerce). AES is included in the ISO/IEC 18033-3 standard. AES is available in many different encryption packages, and is the first (and only) publicly accessible [cipher](https://en.wikipedia.org/wiki/Cipher) approved by the [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) for [top secret](https://en.wikipedia.org/wiki/Classified_information) information when used in an NSA approved cryptographic module (see [Security of AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Security), below).

The name *Rijndael* (Dutch pronunciation: [[ˈrɛindaːl]](https://en.wikipedia.org/wiki/Help:IPA_for_Dutch)) is a play on the names of the two inventors (Joan Daemen and Vincent Rijmen).

## Definitive standards

The Advanced Encryption Standard (AES) is defined in each of:

* FIPS PUB 197: Advanced Encryption Standard (AES)[[6]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-fips-197-6)
* ISO/IEC 18033-3: Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers [[9]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-ISO_IEC_AES-9)

## Description of the cipher

AES is based on a design principle known as a [substitution-permutation network](https://en.wikipedia.org/wiki/Substitution-permutation_network), combination of both substitution and permutation, and is fast in both software and hardware.[[10]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-10) Unlike its predecessor DES, AES does not use a [Feistel network](https://en.wikipedia.org/wiki/Feistel_network). AES is a variant of Rijndael which has a fixed [block size](https://en.wikipedia.org/wiki/Block_size_%28cryptography%29) of 128 [bits](https://en.wikipedia.org/wiki/Bit), and a [key size](https://en.wikipedia.org/wiki/Key_size) of 128, 192, or 256 bits. By contrast, the Rijndael specification *per se* is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

AES operates on a 4×4 [column-major order](https://en.wikipedia.org/wiki/Column-major_order) matrix of bytes, termed the *state*, although some versions of Rijndael have a larger block size and have additional columns in the state. Most AES calculations are done in a special [finite field](https://en.wikipedia.org/wiki/Finite_field_arithmetic).

For instance, if there are 16 bytes, b0,b1,...,b15, these bytes are represented as this matrix:


\begin{bmatrix}
b_0 & b_4 & b_8 & b_{12} \\
b_1 & b_5 & b_9 & b_{13} \\
b_2 & b_6 & b_{10} & b_{14} \\
b_3 & b_7 & b_{11} & b_{15}
\end{bmatrix}


The key size used for an AES cipher specifies the number of repetitions of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext. The number of cycles of repetition are as follows:

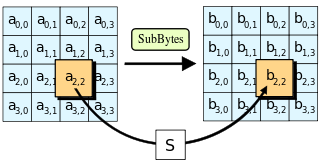
* 10 cycles of repetition for 128-bit keys.
* 12 cycles of repetition for 192-bit keys.
* 14 cycles of repetition for 256-bit keys.

Each round consists of several processing steps, each containing four similar but different stages, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

### High-level description of the algorithm

1. KeyExpansions—round keys are derived from the cipher key using [Rijndael's key schedule](https://en.wikipedia.org/wiki/Rijndael_key_schedule). AES requires a separate 128-bit round key block for each round plus one more.
2. InitialRound
   1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. Rounds
   1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a [lookup table](https://en.wikipedia.org/wiki/Rijndael_S-box).
   2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
   3. MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
   4. AddRoundKey
4. Final Round (no MixColumns)
   1. SubBytes
   2. ShiftRows
   3. AddRoundKey.

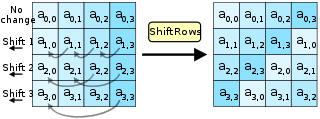
### The SubBytes step

[](https://en.wikipedia.org/wiki/File:AES-SubBytes.svg)

In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, *S*; *bij* = *S(aij)*.

In the SubBytes step, each byte a_{i,j}in the *state* matrix is replaced with a SubByte S(a_{i,j})using an 8-bit [substitution box](https://en.wikipedia.org/wiki/Substitution_box), the [Rijndael S-box](https://en.wikipedia.org/wiki/Rijndael_S-box). This operation provides the non-linearity in the [cipher](https://en.wikipedia.org/wiki/Cipher). The S-box used is derived from the [multiplicative inverse](https://en.wikipedia.org/wiki/Multiplicative_inverse) over [**GF**](https://en.wikipedia.org/wiki/Finite_field)(*28*), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible [affine transformation](https://en.wikipedia.org/wiki/Affine_transformation). The S-box is also chosen to avoid any fixed points (and so is a [derangement](https://en.wikipedia.org/wiki/Derangement)), i.e.,  S(a_{i,j}) \neq a_{i,j} , and also any opposite fixed points, i.e.,  S(a_{i,j}) \oplus a_{i,j} \neq \text{0xFF} . While performing the decryption, Inverse SubBytes step is used, which requires first taking the affine transformation and then finding the multiplicative inverse (just reversing the steps used in SubBytes step).

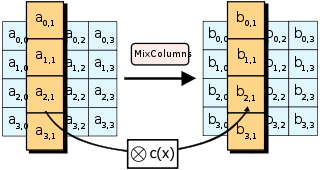
### The ShiftRows step

[](https://en.wikipedia.org/wiki/File:AES-ShiftRows.svg)

In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.

The ShiftRows step operates on the rows of the state; it cyclically shifts the bytes in each row by a certain [offset](https://en.wikipedia.org/wiki/Offset_%28computer_science%29). For AES, the first row is left unchanged. Each byte of the second row is shifted one to the left. Similarly, the third and fourth rows are shifted by offsets of two and three respectively. For blocks of sizes 128 bits and 192 bits, the shifting pattern is the same. Row n is shifted left circular by n-1 bytes. In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state. (Rijndael variants with a larger block size have slightly different offsets). For a 256-bit block, the first row is unchanged and the shifting for the second, third and fourth row is 1 byte, 3 bytes and 4 bytes respectively—this change only applies for the Rijndael cipher when used with a 256-bit block, as AES does not use 256-bit blocks. The importance of this step is to avoid the columns being linearly independent, in which case, AES degenerates into four independent block ciphers.

### The MixColumns step

[](https://en.wikipedia.org/wiki/File:AES-MixColumns.svg)

In the MixColumns step, each column of the state is multiplied with a fixed polynomial *c(x)*.

In the MixColumns step, the four bytes of each column of the state are combined using an invertible [linear transformation](https://en.wikipedia.org/wiki/Linear_transformation). The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes. Together with ShiftRows, MixColumns provides [diffusion](https://en.wikipedia.org/wiki/Diffusion_%28cryptography%29) in the cipher.

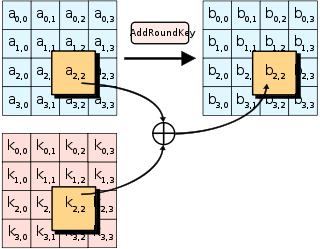
During this operation, each column is transformed using a fixed matrix (matrix multiplied by column gives new value of column in the state):


\begin{bmatrix}
2 & 3 & 1 & 1 \\
1 & 2 & 3 & 1 \\
1 & 1 & 2 & 3 \\
3 & 1 & 1 & 2
\end{bmatrix}


Matrix multiplication is composed of multiplication and addition of the entries. Entries are 8 bit bytes treated as coefficients of polynomial of order x7. Addition is simply XOR. Multiplication is modulo irreducible polynomial x8+x4+x3+x+1. If processed bit by bit then after shifting a conditional [XOR](https://en.wikipedia.org/wiki/Exclusive_or) with 0x1B should be performed if the shifted value is larger than 0xFF (overflow must be corrected by subtraction of generating polynomial). These are special cases of the usual multiplication in **GF**(*28*).

In more general sense, each column is treated as a polynomial over **GF**(*28*) and is then multiplied modulo x4+1 with a fixed polynomial c(x) = 0x03 · x3 + x2 + x + 0x02. The coefficients are displayed in their [hexadecimal](https://en.wikipedia.org/wiki/Hexadecimal) equivalent of the binary representation of bit polynomials from **GF**(2)[x]. The MixColumns step can also be viewed as a multiplication by the shown particular [MDS matrix](https://en.wikipedia.org/wiki/MDS_matrix) in the [finite field](https://en.wikipedia.org/wiki/Finite_field) **GF**(*28*). This process is described further in the article [Rijndael mix columns](https://en.wikipedia.org/wiki/Rijndael_mix_columns).

### The AddRoundKey step

[](https://en.wikipedia.org/wiki/File:AES-AddRoundKey.svg)

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the [XOR](https://en.wikipedia.org/wiki/Exclusive_or) operation (⊕).

In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main [key](https://en.wikipedia.org/wiki/Key_%28cryptography%29) using [Rijndael's key schedule](https://en.wikipedia.org/wiki/Rijndael_key_schedule); each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise [XOR](https://en.wikipedia.org/wiki/Exclusive_or).

### Optimization of the cipher

On systems with 32-bit or larger words, it is possible to speed up execution of this cipher by combining the SubBytes and ShiftRows steps with the MixColumns step by transforming them into a sequence of table lookups. This requires four 256-entry 32-bit tables, and utilizes a total of four kilobytes (4096 bytes) of memory — one kilobyte for each table. A round can then be done with 16 table lookups and 12 32-bit exclusive-or operations, followed by four 32-bit exclusive-or operations in the AddRoundKey step.[[11]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-11)

If the resulting four-kilobyte table size is too large for a given target platform, the table lookup operation can be performed with a single 256-entry 32-bit (i.e. 1 kilobyte) table by the use of circular rotates.

Using a byte-oriented approach, it is possible to combine the SubBytes, ShiftRows, and MixColumns steps into a single round operation.

## Security

Until May 2009, the only successful published attacks against the full AES were [side-channel attacks](https://en.wikipedia.org/wiki/Side-channel_attack) on some specific implementations. The [National Security Agency](https://en.wikipedia.org/wiki/National_Security_Agency) (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data. In June 2003, the U.S. Government announced that AES could be used to protect [classified information](https://en.wikipedia.org/wiki/Classified_information):

The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths. The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.[[13]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-13)

AES has 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. By 2006, the best known attacks were on 7 rounds for 128-bit keys, 8 rounds for 192-bit keys, and 9 rounds for 256-bit keys.

### Known attacks

For cryptographers, a [cryptographic](https://en.wikipedia.org/wiki/Cryptanalysis) "break" is anything faster than a [brute force](https://en.wikipedia.org/wiki/Brute-force_attack)—performing one trial decryption for each key (see [Cryptanalysis](https://en.wikipedia.org/wiki/Cryptanalysis#Computational_resources_required)). This includes results that are infeasible with current technology. The largest successful publicly known [brute force attack](https://en.wikipedia.org/wiki/Brute_force_attack) against any block-cipher encryption was against a 64-bit [RC5](https://en.wikipedia.org/wiki/RC5) key by [distributed.net](https://en.wikipedia.org/wiki/Distributed.net) in 2006.[[15]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-ZD20060430-15)

AES has a fairly simple algebraic description.[[16]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-16) In 2002, a theoretical attack, termed the "[XSL attack](https://en.wikipedia.org/wiki/XSL_attack)", was announced by [Nicolas Courtois](https://en.wikipedia.org/wiki/Nicolas_Courtois) and [Josef Pieprzyk](https://en.wikipedia.org/wiki/Josef_Pieprzyk), purporting to show a weakness in the AES algorithm due to its simple description.[[17]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-17) Since then, other papers have shown that the attack as originally presented is unworkable; see [XSL attack on block ciphers](https://en.wikipedia.org/wiki/XSL_attack#Application_to_block_ciphers).

During the AES process, developers of competing algorithms wrote of Rijndael, "...we are concerned about [its] use...in security-critical applications."[[18]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-rijndael-algebraic-18) However, in October 2000 at the end of the AES selection process, [Bruce Schneier](https://en.wikipedia.org/wiki/Bruce_Schneier), a developer of the competing algorithm [Twofish](https://en.wikipedia.org/wiki/Twofish), wrote that while he thought successful academic attacks on Rijndael would be developed someday, he does not "believe that anyone will ever discover an attack that will allow someone to read Rijndael traffic."[[19]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-19)

On July 1, 2009, Bruce Schneier blogged[[20]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-20) about a [related-key attack](https://en.wikipedia.org/wiki/Related-key_attack) on the 192-bit and 256-bit versions of AES, discovered by [Alex Biryukov](https://en.wikipedia.org/wiki/Alex_Biryukov) and Dmitry Khovratovich,[[21]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-21) which exploits AES's somewhat simple key schedule and has a complexity of 2119. In December 2009 it was improved to 299.5. This is a follow-up to an attack discovered earlier in 2009 by Alex Biryukov, Dmitry Khovratovich, and Ivica Nikolić, with a complexity of 296 for one out of every 235 keys.[[22]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-22) However, related-key attacks are not of concern in any properly designed cryptographic protocol, as properly designed software will not use related-keys.[*[citation needed](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed" \o "Wikipedia:Citation needed)*]

Another attack was blogged by Bruce Schneier[[23]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-23) on July 30, 2009 and released as a preprint[[24]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-24) on August 3, 2009. This new attack, by Alex Biryukov, Orr Dunkelman, Nathan Keller, Dmitry Khovratovich, and [Adi Shamir](https://en.wikipedia.org/wiki/Adi_Shamir), is against AES-256 that uses only two related keys and 239 time to recover the complete 256-bit key of a 9-round version, or 245 time for a 10-round version with a stronger type of related subkey attack, or 270 time for an 11-round version. 256-bit AES uses 14 rounds, so these attacks aren't effective against full AES.

In November 2009, the first [known-key distinguishing attack](https://en.wikipedia.org/wiki/Known-key_distinguishing_attack) against a reduced 8-round version of AES-128 was released as a preprint.[[25]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-25) This known-key distinguishing attack is an improvement of the rebound or the start-from-the-middle attacks for AES-like permutations, which view two consecutive rounds of permutation as the application of a so-called Super-Sbox. It works on the 8-round version of AES-128, with a time complexity of 248, and a memory complexity of 232. 128-bit AES uses 10 rounds, so this attack isn't effective against full AES-128.

In July 2010 Vincent Rijmen published an ironic paper on "chosen-key-relations-in-the-middle" attacks on AES-128.[[26]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-26)

The first [key-recovery attacks](https://en.wikipedia.org/wiki/Key-recovery_attack) on full AES were due to Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger, and were published in 2011.[[27]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-27) The attack is a [biclique attack](https://en.wikipedia.org/wiki/Biclique_attack) and is faster than brute force by a factor of about four. It requires 2126.2 operations to recover an AES-128 key. For AES-192 and AES-256, 2190.2 and 2254.6 operations are needed, respectively. This result has been further improved to 2126.0 for AES-128, 2189.9 for AES-192 and 2254.3 for AES-256,[[28]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-:0-28) which are the current best results in key recovery attack against AES.

This is a very small gain, as a 126-bit key (instead of 128-bits) would still take billions of years to brute force on current and foreseeable hardware. Also, the authors calculate the best attack using their technique on AES with a 128 bit key requires storing 288 bits of data (which later has been improved to 256 [[28]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-:0-28) ). That works out to about 38 trillion terabytes of data, which is more than all the data stored on all the computers on the planet. As such this is a theoretical attack that has no practical implication on AES security.[[29]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-29)

According to the [Snowden documents](https://en.wikipedia.org/wiki/Edward_Snowden#Global_surveillance_disclosures), the NSA is doing research on whether a cryptographic attack based on [tau statistic](https://en.wikipedia.org/wiki/Kendall_tau_rank_correlation_coefficient) may help to break AES.[[30]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-30)

As for now, there are no known practical attacks that would allow anyone to read correctly implemented AES encrypted data.

### Side-channel attacks

[Side-channel attacks](https://en.wikipedia.org/wiki/Side-channel_attacks) do not attack the underlying cipher, and thus are not related to security in that context. They rather attack implementations of the cipher on systems which inadvertently leak data. There are several such known attacks on certain implementations of AES.

In April 2005, [D.J. Bernstein](https://en.wikipedia.org/wiki/Daniel_J._Bernstein) announced a cache-timing attack that he used to break a custom server that used [OpenSSL](https://en.wikipedia.org/wiki/OpenSSL)'s AES encryption.[[31]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-bernstein_timing-31) The attack required over 200 million chosen plaintexts.[[32]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-32) The custom server was designed to give out as much timing information as possible (the server reports back the number of machine cycles taken by the encryption operation); however, as Bernstein pointed out, "reducing the precision of the server's timestamps, or eliminating them from the server's responses, does not stop the attack: the client simply uses round-trip timings based on its local clock, and compensates for the increased noise by averaging over a larger number of samples."[[31]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-bernstein_timing-31)

In October 2005, Dag Arne Osvik, [Adi Shamir](https://en.wikipedia.org/wiki/Adi_Shamir) and Eran Tromer presented a paper demonstrating several cache-timing attacks against AES.[[33]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-33) One attack was able to obtain an entire AES key after only 800 operations triggering encryptions, in a total of 65 milliseconds. This attack requires the attacker to be able to run programs on the same system or platform that is performing AES.

In December 2009 an attack on some hardware implementations was published that used [differential fault analysis](https://en.wikipedia.org/wiki/Differential_fault_analysis) and allows recovery of a key with a complexity of 232.[[34]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-34)

In November 2010 Endre Bangerter, David Gullasch and Stephan Krenn published a paper which described a practical approach to a "near real time" recovery of secret keys from AES-128 without the need for either cipher text or plaintext. The approach also works on AES-128 implementations that use compression tables, such as OpenSSL.[[35]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-35) Like some earlier attacks this one requires the ability to run unprivileged code on the system performing the AES encryption, which may be achieved by malware infection far more easily than commandeering the root account.[[36]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-36)

## NIST/CSEC validation

The [Cryptographic Module Validation Program](https://en.wikipedia.org/wiki/CMVP) (CMVP) is operated jointly by the United States Government's [National Institute of Standards and Technology](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) (NIST) Computer Security Division and the [Communications Security Establishment](https://en.wikipedia.org/wiki/Communications_Security_Establishment) (CSE) of the Government of Canada. The use of cryptographic modules validated to NIST [FIPS 140-2](https://en.wikipedia.org/wiki/FIPS_140-2) is required by the United States Government for encryption of all data that has a classification of Sensitive but Unclassified (SBU) or above. From NSTISSP #11, National Policy Governing the Acquisition of Information Assurance: "Encryption products for protecting classified information will be certified by NSA, and encryption products intended for protecting sensitive information will be certified in accordance with NIST FIPS 140-2."[[37]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-cnss.gov-37)

The Government of Canada also recommends the use of [FIPS 140](https://en.wikipedia.org/wiki/FIPS_140) validated cryptographic modules in unclassified applications of its departments.

Although NIST publication 197 ("FIPS 197") is the unique document that covers the AES algorithm, vendors typically approach the CMVP under FIPS 140 and ask to have several algorithms (such as [Triple DES](https://en.wikipedia.org/wiki/Triple_DES) or [SHA1](https://en.wikipedia.org/wiki/SHA1)) validated at the same time. Therefore, it is rare to find cryptographic modules that are uniquely FIPS 197 validated and NIST itself does not generally take the time to list FIPS 197 validated modules separately on its public web site. Instead, FIPS 197 validation is typically just listed as an "FIPS approved: AES" notation (with a specific FIPS 197 certificate number) in the current list of FIPS 140 validated cryptographic modules.

The Cryptographic Algorithm Validation Program (CAVP)[[38]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-38) allows for independent validation of the correct implementation of the AES algorithm at a reasonable cost[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]. Successful validation results in being listed on the [NIST validations page](http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm). This testing is a pre-requisite for the FIPS 140-2 module validation described below. However, successful CAVP validation in no way implies that the cryptographic module implementing the algorithm is secure. A cryptographic module lacking FIPS 140-2 validation or specific approval by the NSA is not deemed secure by the US Government and cannot be used to protect government data.[[37]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-cnss.gov-37)

FIPS 140-2 validation is challenging to achieve both technically and fiscally.[[39]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard#cite_note-openssl-39) There is a standardized battery of tests as well as an element of source code review that must be passed over a period of a few weeks. The cost to perform these tests through an approved laboratory can be significant (e.g., well over $30,000 US)[[39]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-openssl-39) and does not include the time it takes to write, test, document and prepare a module for validation. After validation, modules must be re-submitted and re-evaluated if they are changed in any way. This can vary from simple paperwork updates if the security functionality did not change to a more substantial set of re-testing if the security functionality was impacted by the change.

## Test vectors

Test vectors are a set of known ciphers for a given input and key. [NIST](https://en.wikipedia.org/wiki/NIST) distributes the reference of AES test vectors as [AES Known Answer Test (KAT) Vectors (in ZIP format)](http://csrc.nist.gov/groups/STM/cavp/documents/aes/KAT_AES.zip).

## Performance

High speed and low RAM requirements were criteria of the AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit [smart cards](https://en.wikipedia.org/wiki/Smart_card) to high-performance computers.

On a [Pentium Pro](https://en.wikipedia.org/wiki/Pentium_Pro), AES encryption requires 18 clock cycles per byte,[[40]](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard" \l "cite_note-40) equivalent to a throughput of about 11 MB/s for a 200 MHz processor. On a 1.7 GHz [Pentium M](https://en.wikipedia.org/wiki/Pentium_M) throughput is about 60 MB/s.

On Intel [Core i3](https://en.wikipedia.org/wiki/Core_i3)/[i5](https://en.wikipedia.org/wiki/Core_i5)/[i7](https://en.wikipedia.org/wiki/Core_i7) and [AMD APU](https://en.wikipedia.org/wiki/AMD_APU) and [FX](https://en.wikipedia.org/wiki/AMD_FX) CPUs supporting [AES-NI instruction set](https://en.wikipedia.org/wiki/AES_instruction_set) extensions, throughput can be over 700 MB/s per thread.

SHA-2

**SHA-2** (**Secure Hash Algorithm 2**) is a set of [cryptographic hash functions](https://en.wikipedia.org/wiki/Cryptographic_hash_function) designed by the [NSA](https://en.wikipedia.org/wiki/National_Security_Agency).[[3]](https://en.wikipedia.org/wiki/SHA-2#cite_note-3) SHA stands for [Secure Hash Algorithm](https://en.wikipedia.org/wiki/Secure_Hash_Algorithm). Cryptographic hash functions are mathematical operations run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity. For example, computing the hash of a downloaded file and comparing the result to a previously published hash result can show whether the download has been modified or tampered with.[[4]](https://en.wikipedia.org/wiki/SHA-2#cite_note-4) A key aspect of cryptographic hash functions is their [collision resistance](https://en.wikipedia.org/wiki/Collision_resistance): nobody should be able to find two different input values that result in the same hash output.

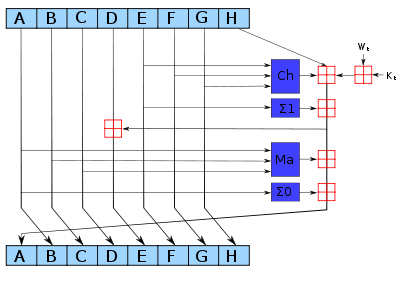
SHA-2 includes significant changes from its predecessor, [SHA-1](https://en.wikipedia.org/wiki/SHA-1). The SHA-2 family consists of six hash functions with [digests](https://en.wikipedia.org/wiki/Cryptographic_hash_function#message_digest) (hash values) that are 224, 256, 384 or 512 bits: **SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256**.

SHA-256 and SHA-512 are novel hash functions computed with 32-bit and 64-bit words, respectively. They use different shift amounts and additive constants, but their structures are otherwise virtually identical, differing only in the number of rounds. SHA-224 and SHA-384 are simply truncated versions of the first two, computed with different initial values. SHA-512/224 and SHA-512/256 are also truncated versions of SHA-512, but the initial values are generated using the method described in FIPS PUB 180-4. SHA-2 was published in 2001 by the [NIST](https://en.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology) as a U.S. federal standard ([FIPS](https://en.wikipedia.org/wiki/Federal_Information_Processing_Standard)). The SHA-2 family of algorithms are patented in US patent 6829355.[[5]](https://en.wikipedia.org/wiki/SHA-2#cite_note-5) The [United States](https://en.wikipedia.org/wiki/United_States) has released the patent under a royalty-free license.[[6]](https://en.wikipedia.org/wiki/SHA-2#cite_note-6)

In 2005, an algorithm emerged for finding SHA-1 collisions in about 2,000-times fewer steps than was previously thought possible.[[7]](https://en.wikipedia.org/wiki/SHA-2#cite_note-7) Although (as of 2015) no example of a SHA-1 collision has been published yet, the security margin left by SHA-1 is weaker than intended, and its use is therefore no longer recommended for applications that depend on collision resistance, such as [digital signatures](https://en.wikipedia.org/wiki/Digital_signature). Although SHA-2 bears some similarity to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2.

Currently, the best public attacks break [preimage resistance](https://en.wikipedia.org/wiki/Preimage_attack) for 52 rounds of SHA-256 or 57 rounds of SHA-512, and [collision resistance](https://en.wikipedia.org/wiki/Collision_attack) for 46 rounds of SHA-256, as shown in the [*Cryptanalysis and validation*](https://en.wikipedia.org/wiki/SHA-2#Cryptanalysis_and_validation) section below.

## Hash standard

[](https://en.wikipedia.org/wiki/File:SHA-2.svg)

One iteration in a SHA-2 family compression function. The blue components perform the following operations:  
    \operatorname{Ch}(E,F,G) = (E \and F) \oplus (\neg E \and G)  
    \operatorname{Ma}(A,B,C) = (A \and B) \oplus (A \and C) \oplus (B \and C)  
    \Sigma_0(A) = (A\!\ggg\!2) \oplus (A\!\ggg\!13) \oplus (A\!\ggg\!22)  
    \Sigma_1(E) = (E\!\ggg\!6) \oplus (E\!\ggg\!11) \oplus (E\!\ggg\!25)  
The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The red \color{red}\boxplusis addition modulo 232.

With the publication of FIPS PUB 180-2, NIST added three additional hash functions in the SHA family. The algorithms are collectively known as SHA-2, named after their digest lengths (in bits): SHA-256, SHA-384, and SHA-512.

The algorithms were first published in 2001 in the draft FIPS PUB 180-2, at which time public review and comments were accepted. In August 2002, FIPS PUB 180-2 became the new [Secure Hash Standard](https://en.wikipedia.org/wiki/Secure_Hash_Standard), replacing FIPS PUB 180-1, which was released in April 1995. The updated standard included the original SHA-1 algorithm, with updated technical notation consistent with that describing the inner workings of the SHA-2 family.[[8]](https://en.wikipedia.org/wiki/SHA-2#cite_note-8)

In February 2004, a change notice was published for FIPS PUB 180-2, specifying an additional variant, SHA-224, defined to match the key length of two-key [Triple DES](https://en.wikipedia.org/wiki/Triple_DES).[[9]](https://en.wikipedia.org/wiki/SHA-2#cite_note-9) In October 2008, the standard was updated in FIPS PUB 180-3, including SHA-224 from the change notice, but otherwise making no fundamental changes to the standard. The primary motivation for updating the standard was relocating security information about the hash algorithms and recommendations for their use to Special Publications 800-107 and 800-57.[[10]](https://en.wikipedia.org/wiki/SHA-2#cite_note-10)[[11]](https://en.wikipedia.org/wiki/SHA-2#cite_note-sp800107-11)[[12]](https://en.wikipedia.org/wiki/SHA-2#cite_note-sp80057-12) Detailed test data and example message digests were also removed from the standard, and provided as separate documents.[[13]](https://en.wikipedia.org/wiki/SHA-2#cite_note-13)

In January 2011, NIST published SP800-131A, which specified a move from the current minimum security of 80-bits (provided by SHA-1) allowable for federal government use until the end of 2013, with 112-bit security (provided by SHA-2) being the minimum requirement current thereafter, and the recommended security level from the publication date.[[14]](https://en.wikipedia.org/wiki/SHA-2#cite_note-14)

In March 2012, the standard was updated in FIPS PUB 180-4, adding the hash functions SHA-512/224 and SHA-512/256, and describing a method for generating initial values for truncated versions of SHA-512. Additionally, a restriction on padding the input data prior to hash calculation was removed, allowing hash data to be calculated simultaneously with content generation, such as a real-time video or audio feed. Padding the final data block must still occur prior to hash output.[[15]](https://en.wikipedia.org/wiki/SHA-2#cite_note-15)

In July 2012, NIST revised SP800-57, which provides guidance for cryptographic key management. The publication disallows creation of digital signatures with a hash security lower than 112-bits after 2013. The previous revision from 2007 specified the cutoff to be the end of 2010.[[12]](https://en.wikipedia.org/wiki/SHA-2#cite_note-sp80057-12) In August 2012, NIST revised SP800-107 in the same manner.[[11]](https://en.wikipedia.org/wiki/SHA-2#cite_note-sp800107-11)

The [NIST hash function competition](https://en.wikipedia.org/wiki/NIST_hash_function_competition) selected a new hash function, [SHA-3](https://en.wikipedia.org/wiki/SHA-3), in 2012.[[16]](https://en.wikipedia.org/wiki/SHA-2#cite_note-nist.gov-16) The SHA-3 algorithm is not derived from SHA-2.

## Applications

For more details on this topic, see [Cryptographic hash function § Applications](https://en.wikipedia.org/wiki/Cryptographic_hash_function#Applications).

The SHA-2 hash function is implemented in some widely used security applications and protocols, including [TLS](https://en.wikipedia.org/wiki/Transport_Layer_Security) and [SSL](https://en.wikipedia.org/wiki/Secure_Sockets_Layer), [PGP](https://en.wikipedia.org/wiki/Pretty_Good_Privacy), [SSH](https://en.wikipedia.org/wiki/Secure_Shell), [S/MIME](https://en.wikipedia.org/wiki/S/MIME), and [IPsec](https://en.wikipedia.org/wiki/IPsec).

SHA-256 is used as part of the process of authenticating [Debian GNU/Linux](https://en.wikipedia.org/wiki/Debian_GNU/Linux) software packages[[17]](https://en.wikipedia.org/wiki/SHA-2#cite_note-17) and in the [DKIM](https://en.wikipedia.org/wiki/DKIM) message signing standard; SHA-512 is part of a system to authenticate archival video from the [International Criminal Tribunal of the Rwandan genocide](https://en.wikipedia.org/wiki/International_Criminal_Tribunal_for_Rwanda).[[18]](https://en.wikipedia.org/wiki/SHA-2#cite_note-18) SHA-256 and SHA-512 are proposed for use in [DNSSEC](https://en.wikipedia.org/wiki/DNSSEC).[[19]](https://en.wikipedia.org/wiki/SHA-2#cite_note-19) Unix and Linux vendors are moving to using 256- and 512-bit SHA-2 for secure password hashing.[[20]](https://en.wikipedia.org/wiki/SHA-2#cite_note-20)

Several [cryptocurrencies](https://en.wikipedia.org/wiki/Cryptocurrency) like [Bitcoin](https://en.wikipedia.org/wiki/Bitcoin) use SHA-256 for verifying transactions and calculating [proof-of-work](https://en.wikipedia.org/wiki/Proof-of-work) or [proof-of-stake](https://en.wikipedia.org/wiki/Proof-of-stake). The rise of [ASIC](https://en.wikipedia.org/wiki/ASIC) SHA-2 accelerator chips has led to the use of [scrypt](https://en.wikipedia.org/wiki/Scrypt)-based proof-of-work schemes.

SHA-1 and SHA-2 are the secure hash algorithms required by law for use in certain [U.S. Government](https://en.wikipedia.org/wiki/U.S._Government) applications, including use within other cryptographic algorithms and protocols, for the protection of sensitive unclassified information. FIPS PUB 180-1 also encouraged adoption and use of SHA-1 by private and commercial organizations. SHA-1 is being retired for most government uses; the U.S. National Institute of Standards and Technology says, "Federal agencies ***should*** stop using SHA-1 for...applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010" (emphasis in original).[[21]](https://en.wikipedia.org/wiki/SHA-2#cite_note-21) NIST's directive that U.S. government agencies must stop uses of SHA-1 after 2010[[22]](https://en.wikipedia.org/wiki/SHA-2#cite_note-22) was hoped to accelerate migration away from SHA-1.

The SHA-2 functions were not quickly adopted, despite better security than SHA-1. Reasons might include lack of support for SHA-2 on systems running Windows XP SP2 or older[[23]](https://en.wikipedia.org/wiki/SHA-2" \l "cite_note-23) and a lack of perceived urgency since SHA-1 collisions have not yet been found. The [Google Chrome](https://en.wikipedia.org/wiki/Google_Chrome) team announced a plan to make their web browser gradually stop honoring SHA-1-dependent TLS certificates over a period from late 2014 and early 2015.

## Cryptanalysis and validation

For a hash function for which *L* is the number of [bits](https://en.wikipedia.org/wiki/Bit) in the [message digest](https://en.wikipedia.org/wiki/Message_digest), finding a message that corresponds to a given message digest can always be done using a [brute force](https://en.wikipedia.org/wiki/Brute-force_attack) search in 2*L* evaluations. This is called a [preimage attack](https://en.wikipedia.org/wiki/Preimage_attack) and may or may not be practical depending on *L* and the particular computing environment. The second criterion, finding two different messages that produce the same message digest, known as a [collision](https://en.wikipedia.org/wiki/Collision_%28computer_science%29), requires on average only 2*L*/2 evaluations using a [birthday attack](https://en.wikipedia.org/wiki/Birthday_attack).

Some of the applications that use cryptographic hashes, such as password storage, are only minimally affected by a [collision attack](https://en.wikipedia.org/wiki/Collision_attack). Constructing a password that works for a given account requires a preimage attack, as well as access to the hash of the original password (typically in the [shadow](https://en.wikipedia.org/wiki/Shadow_password) file) which may or may not be trivial. Reversing password encryption (e.g., to obtain a password to try against a user's account elsewhere) is not made possible by the attacks. (However, even a secure password hash cannot prevent brute-force attacks on [weak passwords](https://en.wikipedia.org/wiki/Password_strength).)

In the case of document signing, an attacker could not simply fake a signature from an existing document—the attacker would have to produce a pair of documents, one innocuous and one damaging, and get the private key holder to sign the innocuous document. There are practical circumstances in which this is possible; until the end of 2008, it was possible to create forged [SSL](https://en.wikipedia.org/wiki/Transport_Layer_Security) certificates using an [MD5](https://en.wikipedia.org/wiki/MD5) collision which would be accepted by widely used web browsers.[[27]](https://en.wikipedia.org/wiki/SHA-2#cite_note-27)

Increased interest in cryptographic hash analysis during the SHA-3 competition produced several new attacks on the SHA-2 family, the best of which are given in the table below. Only the collision attacks are of practical complexity; none of the attacks extend to the full round hash function.

At [FSE](https://en.wikipedia.org/wiki/Fast_Software_Encryption) 2012, researchers at [Sony](https://en.wikipedia.org/wiki/Sony) gave a presentation suggesting pseudo-collision attacks could be extended to 52 rounds on SHA-256 and 57 rounds on SHA-512 by building upon the biclique pseudo-preimage attack

## Examples of SHA-2 variants

Hash values of empty string.

SHA224("")

0x d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f

SHA256("")

0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

SHA384("")

0x 38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b

SHA512("")

0x cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e

SHA512/224("")

0x 6ed0dd02806fa89e25de060c19d3ac86cabb87d6a0ddd05c333b84f4

SHA512/256("")

0x c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a

Even a small change in the message will (with overwhelming probability) result in a mostly different hash, due to the [avalanche effect](https://en.wikipedia.org/wiki/Avalanche_effect). For example, adding a period to the end of the sentence changes 111 out of 224 bits in the hash:

SHA224("[The quick brown fox jumps over the lazy dog](https://en.wikipedia.org/wiki/The_quick_brown_fox_jumps_over_the_lazy_dog)")

0x 730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525

SHA224("[The quick brown fox jumps over the lazy dog](https://en.wikipedia.org/wiki/The_quick_brown_fox_jumps_over_the_lazy_dog).")

0x 619cba8e8e05826e9b8c519c0a5c68f4fb653e8a3d8aa04bb2c8cd4c

## Pseudocode

[Pseudocode](https://en.wikipedia.org/wiki/Pseudocode) for the SHA-256 algorithm follows. Note the great increase in mixing between bits of the w[16..63] words compared to SHA-1.

*Note 1: All variables are 32 bit unsigned integers and addition is calculated modulo 232*

*Note 2: For each round, there is one round constant k[i] and one entry in the message schedule array w[i], 0 ≤ i ≤ 63*

*Note 3: The compression function uses 8 working variables, a through h*

*Note 4: Big-endian convention is used when expressing the constants in this pseudocode,*

*and when parsing message block data from bytes to words, for example,*

*the first word of the input message "abc" after padding is 0x61626380*

*Initialize hash values:*

(first 32 bits of the fractional parts of the square roots of the first 8 primes 2..19):

h0 := 0x6a09e667

h1 := 0xbb67ae85

h2 := 0x3c6ef372

h3 := 0xa54ff53a

h4 := 0x510e527f

h5 := 0x9b05688c

h6 := 0x1f83d9ab

h7 := 0x5be0cd19

*Initialize array of round constants:*

(first 32 bits of the *fractional parts* of the cube roots of the first 64 primes 2..311):

k[0..63] :=

0x428a2f98, 0x71374491, 0xb5c0fbcf, 0xe9b5dba5, 0x3956c25b, 0x59f111f1, 0x923f82a4, 0xab1c5ed5,

0xd807aa98, 0x12835b01, 0x243185be, 0x550c7dc3, 0x72be5d74, 0x80deb1fe, 0x9bdc06a7, 0xc19bf174,

0xe49b69c1, 0xefbe4786, 0x0fc19dc6, 0x240ca1cc, 0x2de92c6f, 0x4a7484aa, 0x5cb0a9dc, 0x76f988da,

0x983e5152, 0xa831c66d, 0xb00327c8, 0xbf597fc7, 0xc6e00bf3, 0xd5a79147, 0x06ca6351, 0x14292967,

0x27b70a85, 0x2e1b2138, 0x4d2c6dfc, 0x53380d13, 0x650a7354, 0x766a0abb, 0x81c2c92e, 0x92722c85,

0xa2bfe8a1, 0xa81a664b, 0xc24b8b70, 0xc76c51a3, 0xd192e819, 0xd6990624, 0xf40e3585, 0x106aa070,

0x19a4c116, 0x1e376c08, 0x2748774c, 0x34b0bcb5, 0x391c0cb3, 0x4ed8aa4a, 0x5b9cca4f, 0x682e6ff3,

0x748f82ee, 0x78a5636f, 0x84c87814, 0x8cc70208, 0x90befffa, 0xa4506ceb, 0xbef9a3f7, 0xc67178f2

*Pre-processing:*

append the bit '1' to the message

append k bits '0', where k is the minimum number >= 0 such that the resulting message

length (modulo 512 in *bits*) is 448.

append length of message (without the '1' bit or padding), in *bits*, as 64-bit big-endian integer

(this will make the entire post-processed length a multiple of 512 bits)

*Process the message in successive 512-bit chunks:*

break message into 512-bit chunks

**for** each chunk

create a 64-entry message schedule array w[0..63] of 32-bit words

*(The initial values in w[0..63] don't matter, so many implementations zero them here)*

copy chunk into first 16 words w[0..15] of the message schedule array

*Extend the first 16 words into the remaining 48 words w[16..63] of the message schedule array:*

**for** i **from** 16 to 63

s0 := (w[i-15] **rightrotate** 7) **xor** (w[i-15] **rightrotate** 18) **xor** (w[i-15] **rightshift** 3)

s1 := (w[i-2] **rightrotate** 17) **xor** (w[i-2] **rightrotate** 19) **xor** (w[i-2] **rightshift** 10)

w[i] := w[i-16] **+** s0 **+** w[i-7] **+** s1

*Initialize working variables to current hash value:*

a := h0

b := h1

c := h2

d := h3

e := h4

f := h5

g := h6

h := h7

*Compression function main loop:*

**for** i **from** 0 to 63

S1 := (e **rightrotate** 6) **xor** (e **rightrotate** 11) **xor** (e **rightrotate** 25)

ch := (e **and** f) **xor** ((**not** e) **and** g)

temp1 := h **+** S1 **+** ch **+** k[i] **+** w[i]

S0 := (a **rightrotate** 2) **xor** (a **rightrotate** 13) **xor** (a **rightrotate** 22)

maj := (a **and** b) **xor** (a **and** c) **xor** (b **and** c)

temp2 := S0 **+** maj

h := g

g := f

f := e

e := d **+** temp1

d := c

c := b

b := a

a := temp1 **+** temp2

*Add the compressed chunk to the current hash value:*

h0 := h0 **+** a

h1 := h1 **+** b

h2 := h2 **+** c

h3 := h3 **+** d

h4 := h4 **+** e

h5 := h5 **+** f

h6 := h6 **+** g

h7 := h7 **+** h

*Produce the final hash value (big-endian):*

digest := hash := h0 **append** h1 **append** h2 **append** h3 **append** h4 **append** h5 **append** h6 **append** h7

**MCRYPT\_MODE\_CBC** (cipher block chaining) is especially suitable for encrypting files where the security is increased over ECB significantly.

# mcrypt\_encrypt

(PHP 4 >= 4.0.2, PHP 5, PHP 7)

mcrypt\_encrypt — Encrypts plaintext with given parameters

### Description [¶](http://php.net/manual/en/function.mcrypt-encrypt.php#refsect1-function.mcrypt-encrypt-description)

string **mcrypt\_encrypt** ( string $cipher , string $key , string $data , string $mode [, string $iv ] )

Encrypts the data and returns it.

### Parameters [¶](http://php.net/manual/en/function.mcrypt-encrypt.php#refsect1-function.mcrypt-encrypt-parameters)

cipher

One of the **MCRYPT\_ciphername** constants, or the name of the algorithm as string.

key

The key with which the data will be encrypted. If the provided key size is not supported by the cipher, the function will emit a warning and return **FALSE**

data

The data that will be encrypted with the given cipher and mode. If the size of the data is not n \* blocksize, the data will be padded with '\0'.

The returned crypttext can be larger than the size of the data that was given by data.

mode

One of the **MCRYPT\_MODE\_modename** constants, or one of the following strings: "ecb", "cbc", "cfb", "ofb", "nofb" or "stream".

iv

Used for the initialization in CBC, CFB, OFB modes, and in some algorithms in STREAM mode. If the provided IV size is not supported by the chaining mode or no IV was provided, but the chaining mode requires one, the function will emit a warning and return **FALSE**.

### Return Values [¶](http://php.net/manual/en/function.mcrypt-encrypt.php#refsect1-function.mcrypt-encrypt-returnvalues)

Returns the encrypted data as a string or **FALSE** on failure.

### Changelog [¶](http://php.net/manual/en/function.mcrypt-encrypt.php" \l "refsect1-function.mcrypt-encrypt-changelog)

| **Version** | **Description** |
| --- | --- |
| 5.6.0 | Invalid key and iv sizes are no longer accepted. **mcrypt\_encrypt()** will now throw a warning and return **FALSE** if the inputs are invalid. Previously keys and IVs were padded with '\0' bytes to the next valid size. |

### Examples [¶](http://php.net/manual/en/function.mcrypt-encrypt.php#refsect1-function.mcrypt-encrypt-examples)

**Example #1 mcrypt\_encrypt() Example**

<?php  
    # --- ENCRYPTION ---  
  
    # the key should be random binary, use scrypt, bcrypt or PBKDF2 to  
    # convert a string into a key  
    # key is specified using hexadecimal  
    $key = pack('H\*', "bcb04b7e103a0cd8b54763051cef08bc55abe029fdebae5e1d417e2ffb2a00a3");  
      
    # show key size use either 16, 24 or 32 byte keys for AES-128, 192  
    # and 256 respectively  
    $key\_size =  strlen($key);  
    echo "Key size: " . $key\_size . "\n";  
      
    $plaintext = "This string was AES-256 / CBC / ZeroBytePadding encrypted.";  
  
    # create a random IV to use with CBC encoding  
    $iv\_size = mcrypt\_get\_iv\_size(MCRYPT\_RIJNDAEL\_128, MCRYPT\_MODE\_CBC);  
    $iv = mcrypt\_create\_iv($iv\_size, MCRYPT\_RAND);  
      
    # creates a cipher text compatible with AES (Rijndael block size = 128)  
    # to keep the text confidential   
    # only suitable for encoded input that never ends with value 00h  
    # (because of default zero padding)  
    $ciphertext = mcrypt\_encrypt(MCRYPT\_RIJNDAEL\_128, $key,  
                                 $plaintext, MCRYPT\_MODE\_CBC, $iv);  
  
    # prepend the IV for it to be available for decryption  
    $ciphertext = $iv . $ciphertext;  
      
    # encode the resulting cipher text so it can be represented by a string  
    $ciphertext\_base64 = base64\_encode($ciphertext);  
  
    echo  $ciphertext\_base64 . "\n";  
  
    # === WARNING ===  
  
    # Resulting cipher text has no integrity or authenticity added  
    # and is not protected against padding oracle attacks.  
      
    # --- DECRYPTION ---  
      
    $ciphertext\_dec = base64\_decode($ciphertext\_base64);  
      
    # retrieves the IV, iv\_size should be created using mcrypt\_get\_iv\_size()  
    $iv\_dec = substr($ciphertext\_dec, 0, $iv\_size);  
      
    # retrieves the cipher text (everything except the $iv\_size in the front)  
    $ciphertext\_dec = substr($ciphertext\_dec, $iv\_size);  
  
    # may remove 00h valued characters from end of plain text  
    $plaintext\_dec = mcrypt\_decrypt(MCRYPT\_RIJNDAEL\_128, $key,  
                                    $ciphertext\_dec, MCRYPT\_MODE\_CBC, $iv\_dec);  
      
    echo  $plaintext\_dec . "\n";  
?>

The above example will output:

Key size: 32

ENJW8mS2KaJoNB5E5CoSAAu0xARgsR1bdzFWpEn+poYw45q+73az5kYi4j+0haevext1dGrcW8Qi59txfCBV8BBj3bzRP3dFCp3CPQSJ8eU=

This string was AES-256 / CBC / ZeroBytePadding encrypted.

**3.1.4.5 MINIMUM HARDWARE AND SOFTWARE REQUIREMENTS**

**Minimum hardware requirements for the Server:**

1. Intel Pentium 4 / AMD Athlon x64 processor, 2 GHz+

2. 100 MB Free Disk Space

3. 256 MB RAM

4. 800 x 600 Display Resolution

5. Ethernet Controller, etc.

**Minimum Hardware Requirements for the Client:**

1. Intel Pentium 4 / AMD Athlon x64 Processor 2GHz+

2. 100 MB Free Disk Space

3. 256 MB RAM

4. 800 x 600 Display Resolution

5. Ethernet Controller

6. Any GPRS / Internet Enabled Mobile

7. Internet Connection

**Minimum Software Requirements for Server:**

1. Operating System: Win XP and above or Linux Distribution

2. Web Browser: Mozilla Firefox, Google Chrome, Internet Explorer 8+, etc.

3. WAMP Server: Windows Apache MySQL PHP

**Minimum Software Requirements for Client:**

1. Operating Systems: Windows, OS X, JAVA Based Mobile, Android OS, Symbian, etc.

2. Web Browser: Mozilla Firefox, Google Chrome, Internet Explorer 8+

**SYSTEM DESIGN**

Systems Design is the process of defining the architecture, components, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

The entire system was designed with one objective in mind, Simplicity. Simplicity was the mantra behind the entire designing process. Right from designing the architecture of the site to designing the final layouts and the registration modules, the approach to make the website and the web application hassle free and convenient for user registration was the ultimate approach.

Few of the very generic models describing the sequence of actions followed by different actors in the model are discussed below. The first of the models is the use case diagram of the Web application:

Apache is developed and maintained by an open community of developers under the auspices of the Apache Software Foundation. Most commonly used on a Unix-like system (usually Linux), the software is available for a wide variety of operating systems, including Unix, FreeBSD, Linux, Solaris, Novell NetWare, OS X, Microsoft Windows, OS/2, TPF, OpenVMS and eComStation. Released under the Apache License, Apache is free and open-source software.

As of June 2013, Apache was estimated to serve 54.2% of all active Web sites and 53.3% of the top servers across all domains

**SYSTEM IMPLEMENTATION AND TESTING**

4.1 SETTING ENVIRONMENT AND IMPLEMENTATION DETAILS

After the entire designing, layout, content, HTML production and programming is done it is now time to deploy the system in real time and test it for bugs. Not only this, after the system is implemented in real time, the responsibility of the designers increase manifold. There are many responsibilities at the designer’s end, such as to provide a bug free software to the clients.

Linux is typically a good match for web hosting servers and applications because of its stability, the savings in running multiple servers without licensing costs, and the flexibility to customize code and applications for specific site or infrastructure needs.

Linux based hosting has a few key advantages over Windows based hosting:

1. Open source platform where it can be improved or modified.

2. Allows other open source platform such as database applications or scripting software (MySQL)

3. It is based on the GNU (General Public License)

4. It is inexpensive

5. Known for its stability and security.

Since Windows is a proprietary operating system, it has fixed number of web developers and programmers working on improving and extending the code base. On the other hand, Linux has a worldwide army of open-source developers who enthusiastically contribute towards making the operating system as secure, fast and user-friendly as possible. This is one big reason why WordPress applications dominate the blogging and content management system (CMS) landscape. WordPress is not only easy to use, it runs incredibly smoothly on a Linux hosting platform.