# **Mod 5 / MIS**

# **Grid Computing**

·**Grid Computing** can be defined as a network of computers working together to perform a task that would rather be difficult for a single machine. All machines on that network work under the same protocol to act as a virtual supercomputer. The task that they work on may include analyzing huge datasets or simulating situations that require high computing power. Computers on the network contribute resources like processing power and storage capacity to the network.

Grid Computing is a subset of distributed computing, where a virtual supercomputer comprises machines on a network connected by some bus, mostly Ethernet or sometimes the Internet. It can also be seen as a form of [Parallel Computing](https://www.geeksforgeeks.org/introduction-to-parallel-computing/) where instead of many CPU cores on a single machine, it contains multiple cores spread across various locations. The concept of grid computing isn’t new, but it is not yet perfected as there are no standard rules and protocols established and accepted by people.

**Working:**   
A Grid computing network mainly consists of these three types of machines

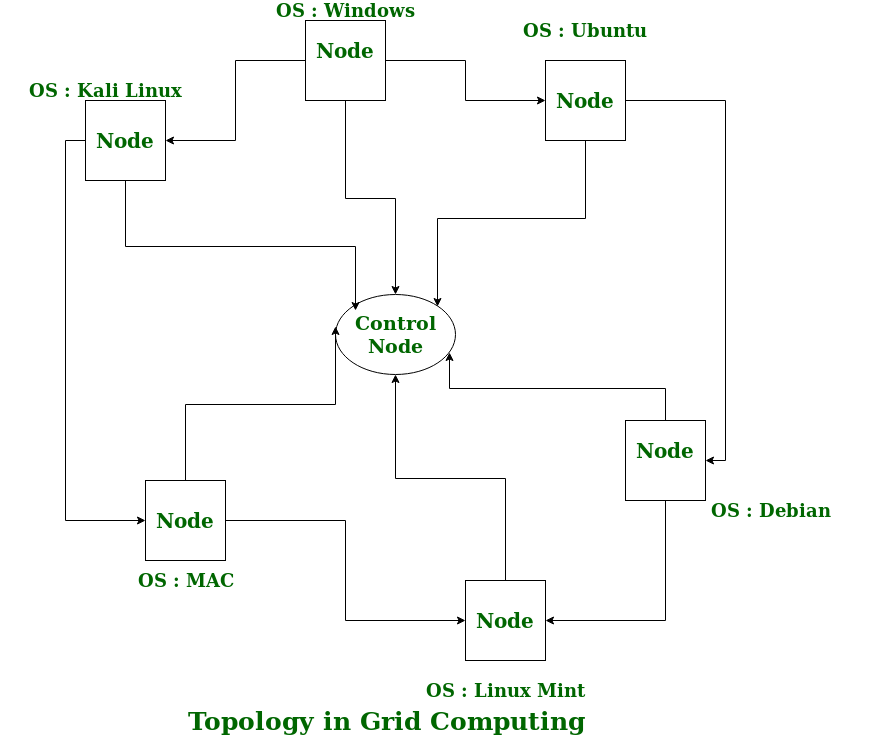
1. **Control Node:** A computer, usually a server or a group of servers which administrates the whole network and keeps the account of the resources in the network pool.
2. **Provider:** The computer contributes its resources to the network resource pool.
3. **User:** The computer that uses the resources on the network.

When a computer makes a request for resources to the control node, the control node gives the user access to the resources available on the network. When it is not in use it should ideally contribute its resources to the network. Hence a normal computer on the node can swing in between being a user or a provider based on its needs. The nodes may consist of machines with similar platforms using the same OS called homogeneous networks, else machines with different platforms running on various different OSs called heterogeneous networks. This is the distinguishing part of grid computing from other distributed computing architectures.

For controlling the network and its resources a software/networking protocol is used generally known as **Middleware**. This is responsible for administrating the network and the control nodes are merely its executors. As a grid computing system should use only unused resources of a computer, it is the job of the control node that any provider is not overloaded with tasks.

Another job of the middleware is to authorize any process that is being executed on the network. In a grid computing system, a provider gives permission to the user to run anything on its computer, hence it is a huge security threat to the network. Hence a middleware should ensure that there is no unwanted task being executed on the network.

The meaning of the term Grid Computing has changed over the years, according to “The Grid: Blueprint for a new computing infrastructure” by Ian Foster and Carl Kesselman published in 1999, the idea was to consume computing power like electricity is consumed from a power grid. This idea is similar to the current concept of cloud computing, whereas now grid computing is viewed as a distributed collaborative network. Currently, grid computing is being used in various institutions to solve a lot of mathematical, analytical, and physics problems.



**Advantages of Grid Computing:**

1. It is not centralized, as there are no servers required, except the control node which is just used for controlling and not for processing.
2. Multiple heterogeneous machines i.e. machines with different Operating Systems can use a single grid computing network.
3. Tasks can be performed parallelly across various physical locations and the users don’t have to pay for them (with money).

**Disadvantages of Grid Computing:**

1. The software of the grid is still in the involution stage.
2. A super-fast interconnect between computer resources is the need of the hour.
3. Licensing across many servers may make it prohibitive for some applications.
4. Many groups are reluctant with sharing resources.
5. Trouble in the control node can come to halt in the whole network.

## **What is green computing?**

Green computing, also known as *green technology*, is the use of computers and other computing devices and equipment in energy-efficient and eco-friendly ways. Organizations that use green computing methods often deploy energy-efficient central processing units (CPUs), servers, peripherals, power systems and other IT equipment. They also focus on reducing resource use and properly disposing of electronic waste.

In many organizations, green computing is a key part of environmental, social and governance ([ESG](https://www.techtarget.com/whatis/definition/environmental-social-and-governance-ESG)) initiatives that focus on the adoption of sustainable and ethical business practices. It also contributes to broader [business sustainability](https://www.techtarget.com/whatis/definition/business-sustainability) efforts, which aim to position companies for ongoing success based on responsible corporate management and strategies.

## **What is included in a green computing strategy?**

Saving money on energy and IT costs is one driving factor for green computing approaches. Government regulations related to energy conservation also drive green efforts. Concern about climate change, combined with internal and external pressure to be environmentally responsible, is a third factor behind the green computing movement.

IT managers typically [focus energy efficiency efforts on data centers](https://www.techtarget.com/searchdatacenter/tip/Four-ways-to-reduce-data-center-power-consumption), as well as separate equipment rooms and data storage areas that use significant amounts of energy or are affected by its use. For example, upgrading IT systems can help by replacing older equipment that often uses more energy and puts out more heat than newer technologies. In addition, [hot and cold aisle setups](https://www.techtarget.com/searchdatacenter/tip/Explore-hot-and-cold-aisle-containment-for-your-data-center) group together data center assets based on energy consumption and temperature output, optimizing the efficiency of heating, ventilation and air conditioning (HVAC) systems.

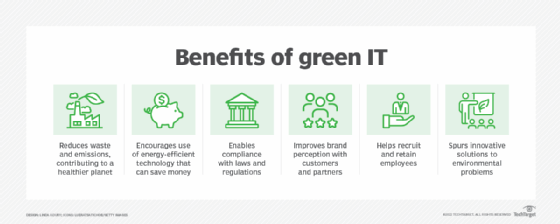
The green computing strategies of companies can also include the following actions, both in and beyond the data center:

* **Deployment of smart technology.** Organizations can use [internet of things](https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT) sensors and artificial intelligence (AI) monitoring tools to collect and analyze information about data centers and create a power usage model. AI-powered tools can also autonomously manage heating, cooling and power in the data center.
* **Powering down IT equipment when it isn't in use.** Servers, CPUs and other devices can be turned off during extended periods of inactivity. In particular, energy-intensive peripherals, such as laser printers, should only be powered up when needed.
* **Strategic scheduling of computer use.** Do computer-related tasks in dedicated blocks of time, leaving hardware off at other times.
* **Energy-efficient computer and display selection.** Laptops use significantly less energy than desktop computers, and liquid-crystal display monitors use less energy and give off less heat than cathode-ray tube monitors.
* **Automated power management.** These features can be set to automatically power down hard drives and monitors after several minutes of inactivity.
* **Temperature check for less cooling.** Newer IT devices can safely run at higher temperatures than older ones, so the data center may not need to be as cool as in the past.
* **Electronic waste disposal.** Dispose of e-waste according to federal, state and local regulations.
* **Alternative energy and cooling opportunities.** Investigate alternative energy sources, such as wind and hydroelectric power, as well as geothermal cooling and other new [methods of cooling data centers](https://www.techtarget.com/searchdatacenter/tip/Data-center-cooling-systems-and-technologies-and-how-they-work).
* **Support for remote work.** The COVID-19 pandemic has spurred many changes in the workplace, including an increase in remote and hybrid work that has led to reduced energy consumption. Besides decreasing the number of people commuting to and from work, it has also cut the number of employees typically present in an organization's facilities, reducing the demand for power and other resources needed to run computers there.

## **The importance of green computing**

The key mission of green computing is to reduce energy consumption. This not only cuts energy costs for organizations, but it also [reduces carbon footprints](https://www.techtarget.com/searchcio/feature/Understand-the-digital-carbon-footprint-of-enterprise-IT), particularly of IT assets. In addition to the cost savings, green approaches to computing can help organizations on regulatory compliance and potentially give them a marketing edge over competitors with both customers and investors.

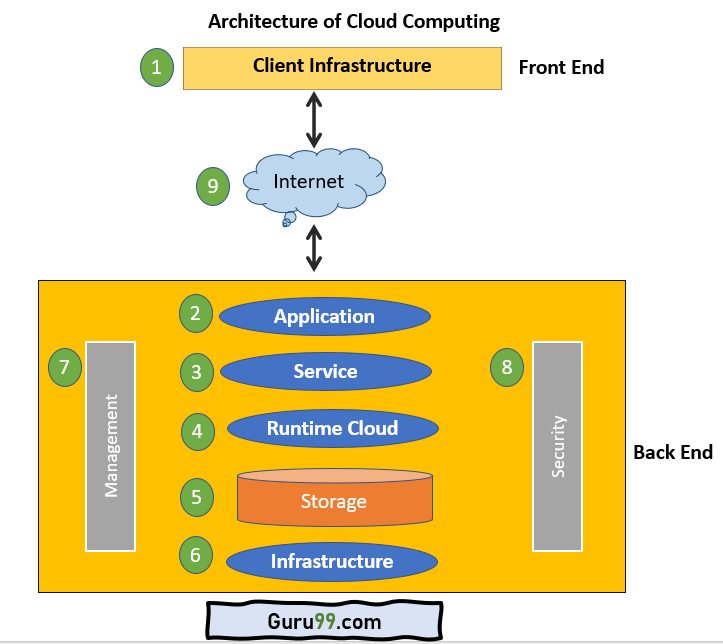
The [environmental impact of IT components](https://www.techtarget.com/searchcio/feature/Environmental-sustainability-considerations-for-IT-teams) is important to consider in the data center design process. Advances in energy management and energy conservation have made IT systems and other computing resources highly energy-efficient. Green design of data centers, [office space and](https://www.techtarget.com/searchhrsoftware/feature/Sustainability-ideas-for-hybrid-offices) other facilities that consume high amounts of energy has become a key part of new construction and building upgrades to make them more environmentally sustainable.

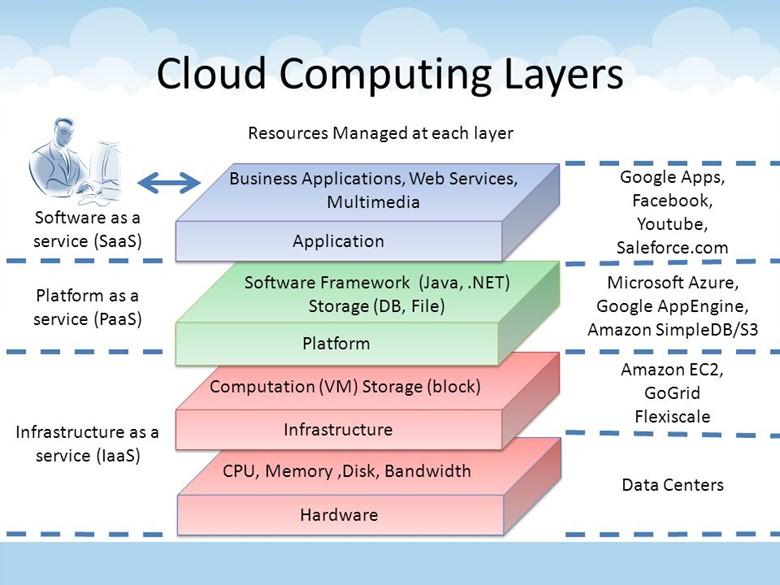
That includes the use of energy-efficient HVAC, power and lighting systems, and a variety of ancillary equipment. For example, many [data center components](https://www.techtarget.com/searchdatacenter/How-to-design-and-build-a-data-center) have a sleep mode that reduces power use or completely shuts down a system during times of low or no use. Also, most IT equipment vendors support green manufacturing practices. The U.S. government's Energy Star logo is an important metric when selecting IT equipment and data center elements.

Another important consideration with green computing and the related concept of [green IT](https://www.techtarget.com/searchcio/definition/green-IT-green-information-technology) is their potential to reduce an organization's use of fossil fuels. This helps lower the amount of pollution released into the atmosphere and water sources -- such reduced emissions have been shown to have positive effects on weather, air pollution and water quality.

**Cloud computing** is the on-demand delivery of IT resources through the internet with pay-to-use charges.

Instead of buying and maintaining computer products and services, you can pay to use a cloud computing service. It saves you the time, effort, and cost of doing it all by yourself!





## **The Three Major Cloud Service Models**

Cloud computing services can be broken down into three models that stack on top of one another:

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a Service (IaaS)

**Software**services are offered under a platform.

**Platform**service is offered under infrastructure as a service.

**Infrastructure**: that's the foundation on which services are built.

## **Types of Cloud Computing**

Cloud computing is not a single piece of technology like a microchip or a cellphone. Rather, it's a system primarily comprised of three services: [software-as-a-service](https://www.investopedia.com/terms/s/software-as-a-service-saas.asp) (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-service (PaaS).

1. **Software-as-a-service (SaaS)** involves the licensure of a software application to customers. Licenses are typically provided through a pay-as-you-go model or on-demand. This type of system can be found in Microsoft Office's 365.1
2. **Infrastructure-as-a-service (IaaS)** involves a method for delivering everything from operating systems to servers and storage through IP-based connectivity as part of an on-demand service. Clients can avoid the need to purchase software or servers, and instead procure these resources in an [outsourced](https://www.investopedia.com/terms/o/outsourcing.asp), on-demand service. Popular examples of the IaaS system include IBM Cloud and Microsoft Azure.12
3. **Platform-as-a-service (PaaS)**is considered the most complex of the three layers of cloud-based computing. PaaS shares some similarities with SaaS, the primary difference being that instead of delivering software online, it is actually a platform for creating software that is delivered via the Internet. This model includes platforms like Salesforce.com and Heroku.3 4

## **The World of Business**

Businesses can employ cloud computing in different ways. Some users maintain all apps and data on the cloud, while others use a hybrid model, keeping certain apps and data on private servers and others on the cloud.When it comes to providing services, the big players in the corporate computing sphere include:

* Google Cloud
* [Amazon Web Services](https://www.investopedia.com/articles/etfs-mutual-funds/080516/4-etfs-fang-stocks-fdnpnqiqqqskyy.asp) (AWS)
* Microsoft Azure
* IBM Cloud
* Alibaba Cloud

Amazon Web Services is 100% public and includes a pay-as-you-go, outsourced model.8 Once you’re on the platform you can sign up for apps and additional services. Microsoft Azure allows clients to keep some data at their own sites. Meanwhile, Alibaba Cloud is a subsidiary of the Alibaba Group.9

## **What Is an Example of Cloud Computing?**

Today, there are several examples of cloud computing applications used by both businesses and individuals. One type of cloud service would be streaming platforms for audio or video, where the actual media files are stored remotely. Another would be data storage platforms like Google Drive, Dropbox, OneDrive, or Box.

## **What Are the Main Types of Cloud Computing?**

The main types of cloud computing services include Infrastructure-as-a-Service (IaaS), Platforms-as-a-Service (PaaS), and Software-as-a-Service (SaaS).10

RedHat. "[Types of cloud computing](https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud#:~:text=There%20are%20also%203%20main,service%20is%20a%20unique%20decision.)."

* IaaS provides IT infrastructure to end-users via the internet and is commonly associated with serverless computing.
* PaaS serves both software and hardware to end-users, who are generally software developers. PaaS allows the user to develop, run, and manage their own apps without having to build and maintain the infrastructure.
* SaaS is a software licensing model, which allows access to software on a subscription basis using external servers without having to download and install them locally.

## **Advantages of Cloud Computing**

As we all know that Cloud computing is trending technology. Almost every company switched their services on the cloud to rise the company growth.

Here, we are going to discuss some important advantages of Cloud Computing-

### **1) Back-up and restore data**

Once the data is stored in the cloud, it is easier to get back-up and restore that data using the cloud.

### **2) Improved collaboration**

Cloud applications improve collaboration by allowing groups of people to quickly and easily share information in the cloud via shared storage.

### **3) Excellent accessibility**

Cloud allows us to quickly and easily access store information anywhere, anytime in the whole world, using an internet connection. An internet cloud infrastructure increases organization productivity and efficiency by ensuring that our data is always accessible.

### **4) Low maintenance cost**

Cloud computing reduces both hardware and software maintenance costs for organizations.

### **5) Mobility**

Cloud computing allows us to easily access all cloud data via mobile.

### **6) IServices in the pay-per-use model**

Cloud computing offers Application Programming Interfaces (APIs) to the users for access services on the cloud and pays the charges as per the usage of service.

### **7) Unlimited storage capacity**

Cloud offers us a huge amount of storing capacity for storing our important data such as documents, images, audio, video, etc. in one place.

### **8) Data security**

Data security is one of the biggest advantages of cloud computing. Cloud offers many advanced features related to security and ensures that data is securely stored and handled.

## **Disadvantages of Cloud Computing**

A list of the disadvantage of cloud computing is given below -

### **1) Internet Connectivity**

As you know, in cloud computing, every data (image, audio, video, etc.) is stored on the cloud, and we access these data through the cloud by using the internet connection. If you do not have good internet connectivity, you cannot access these data. However, we have no any other way to access data from the cloud.

### **2) Vendor lock-in**

Vendor lock-in is the biggest disadvantage of cloud computing. Organizations may face problems when transferring their services from one vendor to another. As different vendors provide different platforms, that can cause difficulty moving from one cloud to another.

### **3) Limited Control -** As we know, cloud infrastructure is completely owned, managed, and monitored by the service provider, so the cloud users have less control over the function and execution of services within a cloud infrastr**ucture.**

### **4) Security**

Although cloud service providers implement the best security standards to store important information. But, before adopting cloud technology, you should be aware that you will be sending all your organization's sensitive information to a third party, i.e., a cloud computing service provider. While sending the data on the cloud, there may be a chance that your organization's information is hacked by Hackers.



## **Bring Your Own Device (BYOD) Meaning**

**BYOD stands for bring your own device**, and the most commonly accepted BYOD meaning is when employees use their own personal devices to connect to the organization's network and access what they need to do their jobs. This includes data and information that could be potentially sensitive or confidential.

The devices used for BYOD could include smartphones, tablets, personal computers, laptops, or USB drives. This offers employees more freedom to use the devices that make them better able to perform day-to-day tasks, which, in the long run, saves employers money. However, BYOD has to be carefully managed with a focus on maintaining security and productivity.

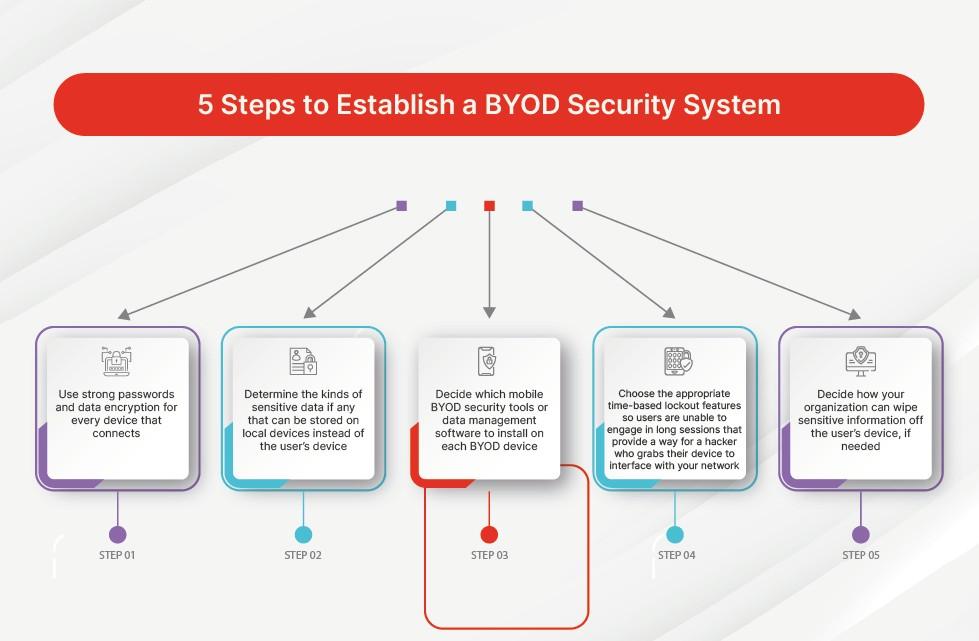
**How Does BYOD Work?**

Bring your own device (BYOD) represents an opportunity for employees to boost their productivity,and when executed using the appropriate safety protocols, a bring-your-own-device policy provides a combination of flexibility and security.

Here is how BYOD works. - **Establishing a BYOD Security System**

In the context of the above BYOD meaning, as is the case with all networking, the first step is to ensure that whenever a user connects to your system, regardless of the device they are using, they do so in a secure manner. Therefore, you need to:

1. Use strong passwords and data encryption for every device that connects
2. Determine the kinds of sensitive data—if any—that can be stored on local devices instead of the user’s device
3. Decide which mobile BYOD security tools or data management software to install on each BYOD device
4. Choose the appropriate time-based lockout features so users are unable to engage in long sessions that provide a way for a hacker who grabs their device to interface with your network
5. Decide how your organization can wipe sensitive information off the user’s device, if needed



### **Which Kinds and How Many Devices Can Users Introduce to Your Network?**

To adequately safeguard your digital assets, figure out which devices to allow to connect. This can prevent a range of less secure devices from accessing your network, such as those with older operating systems with outdated security features the manufacturer no longer supports. The number of devices you allow to access your network is also important because the more that connect, the larger your attack surface.

Here are some questions that could guide your thinking around this decision:

* Is my organization positioned to allow access to legacy devices that are no longer supported by the manufacturer?
* If a device uses an older operating system, do we have measures in place to prevent it from being exploited?
* Should we allow every user to bring multiple devices? Would a limit hamper productivity to the point of making the policy ineffective?
* Are we able to secure a range of mobile phones and tablets—or are our current security protections limited to desktops and laptops? If so, should we upgrade our suite of tools?

**Importance of BYOD Security**

There are several pros and cons of BYOD, and one of the most significant drawbacks is the number of new vulnerabilities it can introduce to your network. BYOD comes with unique data safety challenges. A foundational issue driving the need for BYOD security is you cannot control who has physical access to each device.

For example, when a device is kept inside the office, only those with a physical key, digital key card, and, in some cases, biometric authentication credentials can get their hands on it. But when it is at someone’s home, it may be relatively easy for a hacker to hire a thief to break in and take your employee’s laptop. The hacker can then bring it home and attack it in their personal lab, using a number of online and offline methods.

Also, it is harder to limit the number of viruses and other malware BYOD devices get exposed to because they spend so much time outside your internal firewall protections. This means the number and variety of malicious software floating around each device can be significantly greater than that of an in-house device.

## **What Are the Pros and Cons of Having a BYOD Policy?**

### **Pros**

1. **Faster technology**: With a BYOD policy, an organization benefits from the faster adoption of new technologies, as well as devices that provide faster performance and more computing power. Keeping up with changing technology can be expensive and time-consuming for an IT manager, but if employees bring their own technology, there is no need to constantly update the company’s technology portfolio.
2. **Less time to train employees**: When an employee brings their own device, they typically already know how to use it. Often, transitioning from one operating system to another comes with a learning curve that can increase the amount of time it takes for a new employee to get up to speed. In this way, a BYOD policy can enhance productivity.
3. **Lower up-front costs during onboarding**: If an organization has to purchase a new device, new virus- and malware-protection software, and train new employees regarding how to use the device, the costs can quickly pile up. With BYOD, these costs can be a fraction of what they would be otherwise. With each new employee, an IT team frequently has to provide new security protocols to make interaction with the network secure. Employees often have more than adequate security in place on their own devices, and with a BYOD policy, they can be asked to purchase a security solution before accessing the network.
4. **Employer saves more money**: Constantly purchasing new technology to make sure employees have effective devices can represent a significant cost on a company’s balance sheet. With a BYOD policy, much of the cost was already absorbed by the employee when they purchased the device. In addition, when employees bring their own devices, they are also responsible for upgrading as needed. Not only does this shift the cost away from the company but it also compels the employee to treat their device with more care. When employees take ownership of the maintenance of their device, the company has one less thing to pay for, freeing up crucial overhead.

**Cons - Diaadvantage of BYOD**

1. **Increased complexity for security protocols**: Because each device comes with its own vulnerabilities, including those it may introduce to the organization’s network, you may need to create a more complex arrangement of protocols to [make sure each device is safe](https://www.fortinet.com/content/dam/fortinet/assets/ebook/ebook-nac-in-the-era-of-iot-and-byod.pdf)and does not pose a threat to the network.
2. **Increased security risk**: Each type of device and operating system will require its own security measures so that all endpoints are safe from threats. A device policy that allows employees to bring their own technology may expose the organization to more risk unless each one is properly protected.
3. **Device as a distraction**: Most people have apps on their personal devices that can present significant distractions. Messaging apps, games, and social media apps, for example, can easily grab an employee’s attention when it should be focused on the task at hand. The problem is exacerbated by the specialized app presets that already exist on an employee’s device. These make it easier to log in to social media networks and other cloud-based apps. Because their browser settings and cookies are tailored to their own personal use, when employees are online, they can come across distracting pop-ups and ads customized to grab their attention.
4. **Limited privacy**: With a BYOD policy, both employees and the organization may face privacy issues. For an employee, their personal device, including all its information, data, and passwords, becomes exposed to the companywide network. For an organization, information, data, marketing collateral, and even trade secrets may all have to pass through the personal devices of individual employees, who may not be as discreet as they should be. In addition, each device an employee introduces to the network opens a potential door for malware that could be used to steal sensitive company files.

**Ultra-low-voltage processors (ULV processors)** are a class of microprocessor that are deliberately underclocked to consume less power (typically 17 W or below), at the expense of performance.

Qualcomm's New Snapdragon Chip Promises More Power, Less Battery Drain. If only they named it differently. Qualcomm's chips are powering some of the most powerful Android phones around, and now the company has a new flagship chip that is both faster and more energy efficient than its predecessor.

**Best Processor for Mobile 2023**

| **Rank** | **Processor Name** | **Phone** |
| --- | --- | --- |
| 1 | **Apple A17 Bionic** | Apple iPhone 15 Pro Max |
| 2 | Apple A16 Bionic | Apple iPhone 15 |
| 3 | Snapdragon 8 Gen 3 (Upcoming) | Samsung Galaxy S24 Ultra |
| 4 | Snapdragon 8 Gen 2 | Samsung Galaxy S23 Ultra |

**Autonomic computing (AC)** is distributed computing resources with self-managing characteristics, adapting to unpredictable changes while hiding intrinsic complexity to operators and users.

Autonomic computing is a system that deploys high-level policies to make decisions. It is based on the architecture that is called MAPE that stands for monitor, analyze plan, and execution. The architecture revolves around the idea of a reduction in management costs.

**The goal of Autonomic Computing** is to create systems that are self-managing, meaning they can configure themselves, optimize their own performance, heal themselves if damaged, and protect themselves from threats

Autonomic Computing was originally coined by IBM in 2001 and aims at building computing systems capable of self-management, that is, reacting to internal and external observations without human intervention.

The key advantage of autonomic computing is decreased TCO (Total Cost of Ownership). Breakdowns would be less common with significantly lowering maintenance costs. A very few staffs will be required to operate the networks.

IT infrastructure management – Autonomic computing can also be used in server load balancing, process allocation, memory error correction, automatic upgrading of software and drivers, pre-failure notification, automated device backup and recovery

