G TEC COMPUTER EDUCATION
www.gteceducation.com

G NEWS
The voice of G-TEC

G-TEC COLLEGE FOR ADVANCED STUDIES GCAS
www.gteccollege.com

G-TEC GENSMART ACADEMY
www.gensmartacademy.com

FEB - 2019

G-TEC GROUP OF INSTITUTIONS
Corp. Office: Peace Centre, Singapore 228149

CLOUD COMPUTING

The popular trend in today's technology driven world is 'Cloud Computing'. Cloud computing can be referred to as the storing and accessing of data over the internet rather than your computer's hard drive. This means you don't access the data from either your computer's hard drive or over a dedicated computer network (home or office network). Cloud computing means data is stored at a remote place and is synchronized with other web information.

One prominent example of cloud computing is Office 365 which allows users to store, access, edit their MS Office documents online (in browser) without installing the actual program on their device.

Architecture of Cloud Computing

The architecture of cloud computing comprises of the following components –

- Front-end device
- Back-end platform
- Cloud-based delivery
- Network

Front-end Devices – These are basically the devices that are used by clients to access the data or program using the browser or special applications.

Back-end Platform – There are various computers, servers, virtual machines, etc. that combine to become a back-end platform.

Types of Cloud

The storage options on cloud is in 3 forms

Public Cloud – A service provider makes the clouds available to the general public which is termed as a public cloud. These clouds are accessed through internet by users. These are open to public and their infrastructure is owned and operated by service providers as in case of Google and Microsoft.

Private Cloud – These clouds are dedicated to a particular organization. That particular organization can use the cloud for storing the company's data, hosting business application, etc. The data stored on private cloud can't be shared with other organizations. The cloud is managed either by the organization itself or by the third party.

Hybrid Cloud – When two or more clouds are bound together to offer the advantage of both public and private clouds, they are termed as Hybrid Cloud. Organizations can use private clouds for sensitive application, while public clouds for non-sensitive applications. The hybrid clouds provide flexible, scalable and cost-effective solutions to the organizations.

Advantages and Benefits of Cloud Computing

Trade capital expense for variable expense

Instead of having to invest heavily in data centers and servers before you know how you're going to use them, you can only pay when you consume computing resources, and only pay for how much you consume.

Benefit from massive economies of scale

By using cloud computing, you can achieve a lower variable cost than you can get on your own. Because usage from hundreds of thousands of customers are aggregated in the cloud, providers such as Amazon Web Services can achieve higher economies of scale which translates into lower pay as you go prices

Stop guessing capacity

Eliminate guessing on your infrastructure capacity needs. When you make a capacity decision prior to deploying an application, you often either end up sitting on expensive idle resources or dealing with limited capacity. With cloud computing, these problems go away. You can access as much or as little as you need, and scale up and down as required with only a few minutes notice.

Increase speed and agility

In a cloud computing environment, new IT resources are only ever a click away, which means you reduce the time it takes to make those resources available to your developers from weeks to just minutes. This results in a dramatic increase in agility for the organization, since the cost and time it takes to experiment and develop is significantly lower.

Stop spending money on running and maintaining data centers

Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking and powering servers.

Stop spending money on running and maintaining data centers

Focus on projects that differentiate your business, not the infrastructure. Cloud computing lets you focus on your own customers, rather than on the heavy lifting of racking, stacking and powering servers.

Go global in minutes

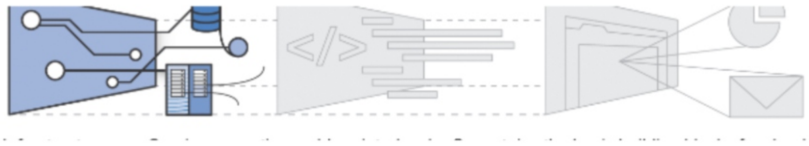
Easily deploy your application in multiple regions around the world with just a few clicks. This means you can provide a lower latency and better experience for your customers simply and at minimal cost.

Types of Cloud Computing

Cloud computing has three main types that are commonly referred to as **Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)**. Selecting the right type of cloud computing for your needs can help you strike the right balance of control and the avoidance of undifferentiated heavy lifting

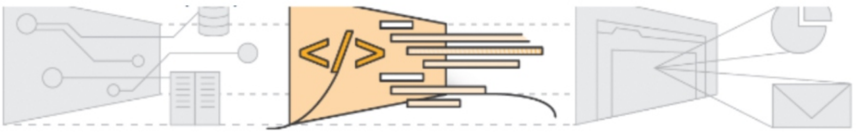
Cloud Computing Models

Infrastructure as a Service (IaaS):



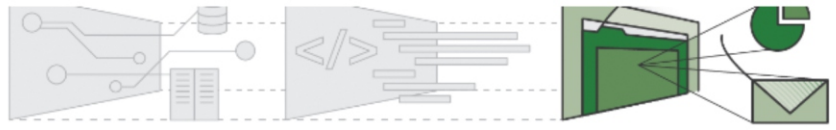
Infrastructure as a Service, sometimes abbreviated as IaaS, contains the basic building blocks for cloud IT and typically provide access to networking features, computers (virtual or on dedicated hardware), and data storage space. Infrastructure as a Service provides you with the highest level of flexibility and management control over your IT resources and is most similar to existing IT resources that many IT departments and developers are familiar with today.

Platform as a Service (PaaS):



Platforms as a service remove the need for organizations to manage the underlying infrastructure (usually hardware and operating systems) and allow you to focus on the deployment and management of your applications. This helps you be more efficient as you don't need to worry about resource procurement, capacity planning, software maintenance, patching, or any of the other undifferentiated heavy lifting involved in running your application.

Software as a Service (SaaS):



Software as a Service provides you with a completed product that is run and managed by the service provider. In most cases, people referring to Software as a Service are referring to end-user applications. With a SaaS offering you do not have to think about how the service is maintained or how the underlying infrastructure is managed; you only need to think about how you will use that particular piece software. A common example of a SaaS application is web-based email where you can send and receive email without having to manage feature additions to the email product or maintaining the servers and operating systems that the email program is running on.

MOST POPULAR SaaS

Amazon Web Services (AWS)

Amazon Web Services (AWS) is a secure cloud services platform, offering compute power, database storage, content delivery and other functionality to help businesses scale and grow. Explore how millions of customers are currently leveraging AWS cloud products and solutions to build sophisticated applications with increased flexibility, scalability and reliability.

Amazon Web Services offers a broad set of global cloud-based products including compute, storage, databases, analytics, networking, mobile, developer tools, management tools, IoT, security and enterprise applications. These services help organizations move faster, lower IT costs, and scale. AWS is trusted by the largest enterprises and the hottest start-ups to power a wide variety of workloads including: web and mobile applications, game development, data processing and warehousing, storage, archive, and many others.

Microsoft Azure

There are many cloud computing platforms offered by different organizations. Windows Azure is one of them, which is provided by Microsoft. Azure can be described as the managed data centers that are used to build, deploy, manage the applications and provide services through a global network. The services provided by Microsoft Azure are PaaS and IaaS. Many programming languages and frameworks are supported by it.

Windows Azure, which was later renamed as Microsoft Azure in 2014, is a cloud computing platform, designed by Microsoft to successfully build, deploy, and manage applications and services through a global network of datacentres. This tutorial explains various features of this flexible platform and provides a step-by-step description of how to use the same.

IT Security

What Is IT Security?

IT security is a set of cybersecurity strategies that prevents unauthorized access to organizational assets such as computers, networks, and data. It maintains the integrity and confidentiality of sensitive information, blocking the access of sophisticated hackers.

What is the need for IT security?

As hackers get smarter, the need to protect your digital assets and network devices is even greater. While providing IT security can be expensive, a significant breach costs an organization far more. Large breaches can jeopardize the health of a small business. During or after an incident, IT security teams can follow an incident response plan as a risk management tool to gain control of the situation.

How do I benefit from IT security?

IT security prevents malicious threats and potential security breaches that can have a huge impact on your organization. When you enter your internal company network, IT security helps ensure only authorized users can access and make changes to sensitive information that resides there. IT security works to ensure the confidentiality of your organization's data.

Types of IT security

Network security

Network security is used to prevent unauthorized or malicious users from getting inside your network. This ensures that usability, reliability, and integrity are uncompromised. This type of security is necessary to prevent a hacker from accessing data inside the network. It also prevents them from negatively affecting your users' ability to access or use the network.Network security has become increasingly challenging as businesses increase the number of endpoints and migrate services to public cloud.

Internet security

Internet security involves the protection of information that is sent and received in browsers, as well as network security involving web-based applications. These protections are designed to monitor incoming internet traffic for malware as well as unwanted traffic. This protection may come in the form of firewalls, antimalware, and antispyware.

Endpoint security

Endpoint security provides protection at the device level. Devices that may be secured by endpoint security include cell phones, tablets, laptops, and desktop computers. Endpoint security will prevent your devices from accessing malicious networks that may be a threat to your organization. Advance malware protection and device management software are examples of endpoint security.

Cloud security

Applications, data, and identities are moving to the cloud, meaning users are connecting directly to the Internet and are not protected by the traditional security stack. Cloud security can help secure the usage of software-as-a-service (SaaS) applications and the public cloud. A cloud-access security broker (CASB), secure Internet gateway (SIG), and cloud-based unified threat management (UTM) can be used for cloud security.

Application security

With application security, applications are specifically coded at the time of their creation to be as secure as possible, to help ensure they are not vulnerable to attacks. This added layer of security involves evaluating the code of an app and identifying the vulnerabilities that may exist within the software.

What are CCTV cameras used for?

CCTV (closed-circuit television) is a TV system in which signals are not publicly distributed but are monitored, primarily for surveillance and security purposes.

CCTV relies on strategic placement of cameras, and observation of the camera's input on monitors somewhere. Because the cameras communicate with monitors and/or video recorders across private coaxial cable runs or wireless communication links, they gain the designation "closed-circuit" to indicate that access to their content is limited by design only to those able to see it.

Older CCTV systems used small, low-resolution black and white monitors with no interactive capabilities. Modern CCTV displays can be color, high-resolution displays and can include the ability to zoom in on an image or track something (or someone) among their features. Talk CCTV allows an overseer to speak to people within range of the camera's associated speakers.

CCTV is commonly used for a variety of purposes, including:

- Maintaining perimeter security in medium- to high-secure areas and installations.
- Observing behavior of incarcerated inmates and potentially dangerous patients in medical facilities.

- Maintaining perimeter security in medium- to high-secure areas and installations.
- Observing behavior of incarcerated inmates and potentially dangerous patients in medical facilities.
- Traffic monitoring.
- Overseeing locations that would be hazardous to a human, for example, highly radioactive or toxic industrial environments.
- Building and grounds security.
- Obtaining a visual record of activities in situations where it is necessary to maintain proper security or access controls (for example, in a diamond cutting or sorting operation; in banks, casinos, or airports).

CCTV is finding increasing use in law-enforcement, for everything from traffic observation (and automated ticketing) to observation of high-crime areas or neighborhoods. Such use of CCTV technology has fueled privacy concerns in many parts of the world, particularly in those areas in the UK and Europe where it has become a routine part of police procedure.

Why Security Cameras Are Important

A residential security system is becoming more and more important due to the increasing crime and theft around us. They are able to provide us with video footage, whether live or recorded, within our property. In fact, thanks to the presence of surveillance systems, undeniable video evidences have led to the incarceration of many criminals. This is the reason why a lot of people are protecting their homes and businesses with security cameras.

The popularity of security cameras have increased in the last decade and due to the advancement of technology, they now come in many shapes and sizes. There are also wired and wireless versions of these security systems. The wireless versions offer much more flexibility as they can be placed almost anywhere.

Security cameras that are internet-ready are a good way of monitoring your home or your business. They can be viewed from almost any location that has a computer with internet connection. This allows owners to keep an eye on their property while they are away. There are even surveillance systems that can notify you through email when movement has been detected.

Security cameras that are equipped with motion sensors give them the capability of detecting movements. Even the slightest movement can trigger these motion sensors to start the video recording process.

Digital Security surveillance cameras are much smaller. Despite their size, they are capable of recording video for a long period. The images and videos they record can be saved and edited in a computer. They have gained in popularity because they have eliminated the need for video tapes as a recording medium.

The presence of security systems have helped in deterring crimes and theft. This reputation has helped them become popular with homes and businesses. Through the years, security surveillance camera systems have become more affordable. For this reason, more and more households and businesses are being equipped with security cameras with the hopes of protecting their properties.

Overall, the importance of a residential security system has become more and more undeniable. There are a lot of intruders who are wary of security cameras and are well aware that they can be easily be tracked by law enforcers if they ever get caught in one. They get discouraged with just the sight of it. One of the major benefits of having a video surveillance system is safety. The installation of surveillance systems gives home owners and business owners a peace of mind.

Different Types Of CCTV Cameras

Bullet Type Cameras are designed for capturing images in a fixed area. These cameras are recognized by their thin and cylindrical design. There are also classifications of Ultra Bullet distinguished by their smaller size and cheaper price.

Dome Cameras, named after the shape of their housing are designed for in-store installations. It works in two ways as it is unobtrusive but visible, thus, it warns people that the area is protected by a CCTV network and gives comfort to its clients for its security.

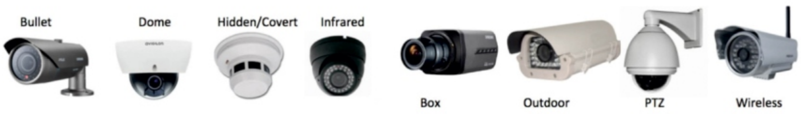
Discreet CCTVs are cameras in disguise, they could look like a fan or any other thing that would not seem suspicious in the area.

Infrared Cameras are designed for evening lookouts. It captures images with the help of its infrared lighting surrounding its lens.

Infrared Cameras are designed for evening lookouts. It captures images with the help of its infrared lighting surrounding its lens.

Day/Night Types are used for 24/7 installation, these cameras compensate light conditions with its wide dynamic range to function in glare, direct sunlight, reflections and strong backlight.

Varifocal Cameras are designed to allow zooming in and out without losing focus on the image.



Network Cameras allow transmission of images through the internet with controlled bandwidth.

Wireless cameras are cameras that may or may not be connected to the internet. These cameras use signaling devices to transmit images from camera to viewing area.

PTZ Cameras or pan-tilt-zoom are cameras that can moved. There are variations of these cameras that are programmable and are manually controllable. This allows viewers to have more freedom and control on viewing things.

High definition cameras are often used in casinos or high risk establishment. With its high resolution lens, capturing images are possible giving viewers a finer detail on taken images.

Fire alarm system

A fire alarm system has a number of devices working together to detect and warn people through visual and audio appliances when smoke, fire, carbon monoxide or other emergencies are present. These alarms may be activated automatically from smoke detectors, and heat detectors or may also be activated via manual fire alarm activation devices such as manual call points or pull stations. Alarms can be either motorized bells or wall mountable sounders or horns. They can also be speaker strobes which sound an alarm, followed by a voice evacuation message which warns people inside the building not to use the elevators. Fire alarm sounders can be set to certain frequencies and different tones including low, medium and high, depending on the country and manufacturer of the device

What is a security system?

The most basic definition of any security system is found in its name. It is literally a means or method by which something is secured through a system of interworking components and devices.In this instance, we're talking about home security systems, which are networks of integrated electronic devices working together with a central control panel to protect against burglars and other potential home intruders.

A typical home security system includes:

- A control panel, which is the primary controller of a home's security system
- Door and window sensors
- Motion sensors, both interior and exterior
- Wired or wireless security cameras
- A high-decibel siren or alarm
- A yard sign and window stickers

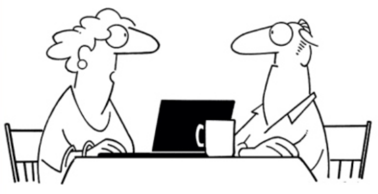
How does a security system work?

Home security systems work on the simple concept of securing entry points into a home with sensors that communicate with a control panel or command center installed in a convenient location somewhere in the home.The sensors are typically placed in doors that lead to and from a house as well as easily accessible windows, particularly any that open, especially those at ground level. Open spaces inside of homes can be secured with motion sensors.

Control Panel: The control panel is the computer that arms and disarms the security systems, communicates with each installed component, sounds the alarm when a security zone is breached, and communicates with an alarm monitoring company.They typically feature a touchpad for easy programming and interaction, is where pass codes are entered to arm and disarm the system, can work on voice commands, and can be programmed to work with wireless remote controls called key fobs

Door and Window Sensors: Door and window sensors are comprised of two parts installed adjacent to each other. One part of the device is installed on the door or window and the other on the door frame or window sill. When a door or window is closed, the two parts of the sensor are joined together, creating a security circuit.When the security system is armed at the control panel, these sensors communicate with it by reporting that the point of entry is secure. Should a monitored door or window suddenly be opened, the security circuit is broken and the control panel interprets this as a breach of a secured zone. A high-decibel alarm is sounded and in most instances the alarm monitoring company is automatically notified.

Smile Corner



When I was a little girl, I had an imaginary friend
Now I have 875 imaginary friends on Facebook

G NEWS

Publisher
Mehroof I. Manalody

Chief Editor
S. Thulaseedharan Pillai
AGM - Operations

Editor
Joseph M Thomas
HOD - Academics

Editorial Board
K.B. Nandakumar (General Manager)
Deepak Padiyath (Vice President & CEO GENSMART)
Ashley George Vaz (Manager Operations)
Sajindas T (Operations Manager)
Saidu Muhammed (Director Operations, GENSMART)
Anwar Sathic (Marketing Manager)
Shibida Ahamed (Technical Manager)
Raihana K (Academic Coordinator)

Email: gnews@gteceducation.com
For internal circulation only

Home Security System

Motion Sensors: These security components, when armed, protect a given space by creating an invisible zone that cannot be breached without sounding an alarm. These are typically used to protect rooms containing valuables, as well as areas less frequented in larger homes.

Surveillance Cameras: Available in both wired and wireless configurations, surveillance cameras can be used in several different ways as part of an overall security system.

Typical uses include monitoring:

- Hard to see or distant areas of your property
- Remote buildings like garages, barns, and workshops
- Entry points, both exterior and interior, like garage doors and front doors

Surveillance cameras can be accessed remotely on computers, smartphones, and tablets. They are often used in this method when homeowners are out of town, to watch for deliveries and other service personnel like caregivers and landscapers, and to monitor the arrival of children after school. They can also be used to record any security breaches, which could result in having footage of a home invasion, including a good look at the burglars and perhaps even the vehicle they drove.

High-decibel Alarm: Loud enough for neighbors to hear, home security alarms serve a few different purposes. First, they alert the people inside the house that a problem occurred. They're also shrill enough to send a burglar running while also notifying nearby neighbors to the situation.

Yard Sign and Window Stickers: On the surface, these items might seem like nothing more than marketing tools for alarm companies, but they play important roles in home security. When you place a security company's sticker in a front window and plant their sign in your front yard, you are telling burglars you home is professionally protected and not a wise choice for an attempted burglary. They are effective at conveying this message and should be used as recommended by the security company.

What Happens when an intrusion occurs?

Security systems are designed to perform certain tasks when a secured zone is breached. What your security systems does in the event of an intrusion depends on the type of system you're using.Professionally Monitored Security Systems: If your security system is professionally monitored by an alarm company, they are alerted when a security problem arises in your home. Along with the high-decibel alarm that sounds, the monitoring company is alerted. A trained security expert might attempt to communicate with the homeowner via the control panel if it's setup for 2-Way Voice communication, or will call the emergency contact number listed on the account.

These types of security systems communicate with the monitoring company in one of several ways, including:

- Over existing home phone lines, which continue to work during power outages when battery backup is in use.
- Wirelessly through cellular radio frequencies like cell phones use, which also continue to work during power outages when battery backup is in use.
- Voice over Internet Protocol (VoIP), which typically doesn't work in a power outage.
- Via the Internet, which also typically does not work in a power outage.

In the event of an actual emergency, the monitoring company will notify the appropriate emergency response personnel in your area. This includes police, firefighters, and paramedics. The monitoring company will also try to maintain communication with you until emergency response teams arrive at your home.

Monitored systems typically allow for the homeowners (or designees) to be notified by text message and email when a security breach occurs.

Non-monitored Security Systems: There are plenty of DIY security systems available today that don't include professionally monitored services. In the event of a home intrusion when this type of security system is installed, a high-decibel alarm sounds (provided one is installed). Contacting police, fire, or other emergency response personnel must be initiated by the homeowner by dialing the appropriate number.These types of systems may or may not allow for text messages or email notifications to be sent to the homeowner in the event of a security breach, depending on the provider and the system you opted for.

Advantages of having a home security system:

When you have a home security system professionally monitored, and advertise this by displaying window stickers and yard signs, you're letting burglars know the likelihood they'll fail and be caught are very high.

Another advantage is the ability to remotely manage your house. With this, you can typically arm and disarm your security system from anywhere in the world via a web-enabled device, monitor who arrives and leaves your home, as well as use a panic button to elicit an instant response from your alarm monitoring company.

Finally, most home insurance companies provide great discounts-up to 20 percent-when you have a home security system in your home.

Access Control System (ACS)

An access control system (ACS) is a type of security that manages and controls who or what is allowed entrance to a system, environment or facility.

It identifies entities that have access to a controlled device or facility based on the validity of their credentials.

An ACS is primarily a physical operation implemented within high security areas, such as data centers, government/military institutes and similar facilities.

Typically, an ACS manages, monitors and controls human access to the protected equipment or facility. Most ACSs are designed to take a user provided credential as input, verify/authenticate privileges using the access control list (ACL) and grant/deny access based on the findings.

For example, using biometric security, an ACS can be used to authorize only legitimate access to a data center facility. The individual must provide his or her thumb print, focal or vocal credentials to an ACS, which is then verified through comparison with its database, and grants access only with valid permission.

Types of Access Control Systems

In brief, access control is used to identify an individual who does a specific job, authenticate them, and then proceed to give that individual only the key to the door or workstation that they need access to and nothing more. Access control systems come in three variations: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC).

1. Discretionary Access Control (DAC)

Discretionary Access Control is a type of access control system that holds the business owner responsible for deciding which people are allowed in a specific location, physically or digitally. DAC is the least restrictive compared to the other systems, as it essentially allows an individual complete control over any objects they own, as well as the programs associated with those objects. The drawback to Discretionary Access Control is the fact that it gives the end user complete control to set security level settings for other users and the permissions given to the end user are inherited into other programs they use which could potentially lead to malware being executed without the end user being aware of it.

2. Mandatory Access Control (MAC)

Mandatory Access Control is more commonly utilized in organizations that require an elevated emphasis on the confidentiality and classification of data (ie. military institutions). MAC doesn't permit owners to have a say in the entities having access in a unit or facility, instead, only the owner and custodian have the management of the access controls. MAC will typically classify all end users and provide them with labels which permit them to gain access through security with established security guidelines.

3. Role-Based Access Control (RBAC)

Also known as Rule-Based Access Control, RBAC is the most demanded in regard to access control systems. Not only is it in high demand among households, RBAC has also become highly sought-after in the business world. In RBAC systems, access is assigned by the system administrator and is stringently based on the subject's role within the household or organization and most privileges are based on the limitations defined by their job responsibilities. So, rather than assigning an individual as a security manager, the security manager position already has access control permissions assigned to it. RBAC makes life much easier because rather than assigning multiple individuals particular access, the system administrator only has to assign access to specific job titles

Choosing the Best Access Control System for Your Organization

As we can see, when it comes to choosing the type of access control system that is most suitable for your organization, there are a number of factors involved. Some of those factors include the nature of your business, security procedures within the organization, and the number of users on the system. Places of business with small or basic applications will probably find Discretionary Access Control to be less complicated and better utilized. If, however, you have highly confidential or sensitive information on your business platform, a Mandatory Access or Role-Based Access Control system are two options you may want to consider.

OUR PRIDE