CHAPTER-8
EMERGING TECHNOLOGIES

8.1. Cloud Computing

Cloud computing simply means the use of computing resources as a service through networks, typically the Internet. The Internet is commonly visualized as clouds; hence the term "cloud computing" for computation done through the Internet. With Cloud Computing, users can access database resources via the Internet from anywhere, for as long as they need, without worrying about any maintenance or management of actual resources. Besides these, databases in cloud may be highly dynamic and scalable. In fact, it is a very independent platform in terms of computing. The best example of cloud computing is Google Apps where any application can be accessed using a browser and it can be deployed on thousands of computer through the Internet.

Cloud computing provides the facility to access shared resources and common infrastructure offering services on demand over the network to perform operations that meet changing business needs. The location of physical resources and devices being accessed are typically not known to the end user. It also provides facilities for users to develop, deploy and manage their applications 'on the cloud', which entails virtualization of resources that maintains and manages itself.

Cloud computing is of particular benefit to small and medium-sized business systems, who wish to completely outsource their data-centre infrastructure; or large companies, who wish to get peak load capacity without incurring the higher cost of building larger data centres internally. In both the instances, service consumers use 'what they need on the Internet' and pay only for 'what they use'

8.2. Cloud vs Grid Computing

Cloud computing evolved from grid computing and provides on-demand resource provisioning. Grid computing may or may not be in the cloud paradigm depending on what type of users are using it. If the users are systems administrators and integrators, they care 'how things are maintained in the cloud'. They upgrade, install, and virtualized servers and applications. If the users are consumers, they do not care 'how things are run in the system'.

Grid computing requires the use of software that can divide and carve out pieces of a program as one large system image to several thousand computers. One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail.

Some pertinent similarities and differences are highlighted as follows:

1) Cloud computing and grid computing both are scalable. Scalability is accomplished through load balancing of application instances running separately on a variety of operating systems and connected through Web services. CPU and network bandwidth is allocated and de-allocated on demand.

2) Both computing types involve multitenancy and multitasking, meaning that many customers can perform different tasks, accessing a single or multiple application instances. Sharing resources among a large pool of users assists in reducing infrastructure costs and peak load capacity. Cloud and grid computing provide Service- Level Agreements (SLAs) for guaranteed uptime availability of, say, 99 percent.

3) While the storage computing in the grid is well suited for data-intensive storage, it is not economically suited for storing objects as small as 1 byte. In a data grid, the amounts of distributed data must be large for maximum benefit. While in cloud computing, we can store an object as low as 1 byte and as large as 5 GB or even several terabytes.

4) A computational grid focuses on computationally intensive operations, while cloud computing offers two types of instances: standard and high-CPU.

8.3. Pertinent Issues

Some of the well-identified issues stand out with cloud computing are described briefly as follows:

1) **Threshold Policy:** In order to test if the program works, develop, or improve and implement, a threshold policy is of immense importance in a pilot study before moving the program to the production environment. Checking how the policy enables to detect sudden increases in the demand and results in the creation of additional instances to fill in the demand. Moreover, to determine how unused resources are to be de- allocated and turned over to other work needs to work out in the context. That is working out thresholds is really a matter of concern and would go a long way to assure the effectiveness.

2) **Interoperability:** If a company outsources or creates applications with one cloud computing vendor, the company may find it difficult to change to another computing vendor that has proprietary APIs and different formats for importing and exporting data. This creates problems of achieving interoperability of applications between two cloud computing vendors. We may need to reformat/reorganize data or change the logic in applications. Although industry cloud-computing standards do not exist for APIs or data import/export, IBM and Amazon Web Services have worked together to make interoperability happen.

3) **Hidden Costs:** Like any such services in prevailing business systems, cloud computing service providers do not reveal 'what hidden costs are'. For instance, companies could incur higher network charges from their service providers for storage and database applications containing terabytes of data in the cloud. This outweighs costs they could save on new infrastructure, training new personnel, or licensing new software. In another instance of incurring network costs, companies, who are far from the location of cloud providers could experience latency, particularly when there is heavy traffic.

4) **Unexpected Behaviour:** Let's suppose that credit card validation application works well at our company's internal data centre. It is important to test the application in the cloud with a pilot study to check for unexpected behaviour. Examples of tests include how the application validates credit cards, and how, in the scenario of the buying crunch, it allocates resources and releases unused resources, turning them over to other work. If the tests show unexpected results of credit card validation or releasing unused resources, we will need to fix the problem before executing or obtaining cloud services from the cloud.

5) **Security Issues:** Security is a major issues relating to cloud computing. Instead of waiting for an outage to occur, consumers should do security testing on their own checking how well a vendor can recover data. Apart from the common testing practices, what one needs primarily to do is to ask for old stored data and check how long it takes for the vendor to recover. If it takes too long to recover, ask the vendor why and how much service credit we would get in different scenarios. Moreover, in such cases, verifying the checksums match with the original data is a requisite.

6) **Software Development in Cloud:** To develop software using high-end databases, the most likely choice is to use cloud server pools at the internal data corporate centre and extend resources temporarily for testing purposes. This allows project managers to control costs, manage security and allocate resources to clouds for a project. The project managers can also assign individual hardware resources to different cloud types: Web development cloud, testing cloud, and production cloud. The cost associated with each cloud type may differ from one another. The cost per hour or usage with the development cloud is most likely lower than the production cloud, as additional features, such as SLA and security, are allocated to the production cloud. The managers can limit projects to certain clouds. For instance, services from portions of the production cloud can be used for the production configuration. Services from the development cloud can be used for development purpose only. To optimize assets at varying stages of the project of software development, the managers can get cost-accounting data by tracking usage by project and user.

7) **Environment Friendly Cloud Computing:** One incentive for cloud computing is that it may be more environment friendly. First, reducing the number of hardware components needed to run applications on the company's internal data centre and replacing them with cloud computing systems reduces energy for running and cooling hardware. By consolidating these systems in remote centres, they can be handled more efficiently as a group.

8.4. Goals of Cloud Computing

The core goals of utilizing a cloud-based IT ecosystem are to pool available resources together into a highly efficient infrastructure whose costs are aligned with what resources are actually used but to the services accessible and available from anywhere at any time.
To meet the requirements, some of the pertinent objectives in order to achieve the goals are as follows:

1) To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;

2) To access services and data from anywhere at any time;

3) To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;

4) To consolidate IT infrastructure into a more integrated and manageable environment;

5) To reduce costs related to IT energy/power consumption;

6) To enable or improve "Anywhere Access" (AA) for ever increasing users; and

7) To enable rapidly provision resources as needed.

8.5. Cloud Computing Architecture

The Cloud Computing Architecture (CCA) of a cloud solution is the structure of the system, which comprises of on-premise and cloud resources, services, middleware, and software components, their geo-location, their externally visible properties and the relationships between them. Cloud architecture typically involves into multiple cloud components communicating with each other over a loose coupling mechanism, such as a messaging queue. Elastic provisioning implies intelligence in the use of tight or loose coupling of cloud resources, services, middleware, and software components.

In the context of cloud computing, protection depends on having the Right Architecture for the Right Application (RARA). Organizations must understand the individual requirements of their applications, and if already using a cloud platform, understand the corresponding cloud architecture. A cloud computing architecture consists of a front end and a back end.

The details are given as follow:

1) **Front End Architecture:** The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.

2) **Back End Architecture:** Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

8.6. Cloud Computing Environment

The cloud computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows

1) **Public Clouds:** This environment can be used by the general public. This includes individuals, corporations and other types of organizations. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called provider clouds. Business models like SaaS (Software-as-a-Service) and public clouds complement each other and enable companies to leverage shared IT resources and services.
   The Advantages of public cloud include the following:
   a) It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
   b) It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.

   Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen.

2) **Private Clouds:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called internal clouds. They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

   The advantages of private clouds include the following:
   a) They improve average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
   b) High levels of automation is largely responsible for reducing operations costs and administrative overheads

   Moreover, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently.

3) **Hybrid Clouds:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. It is typically offered in either of two ways. A vendor has a private cloud and form a partnership with a public cloud provider or a public cloud provider forms a platforms. partnership/franchise with a vendor that provides private cloud platforms

8.7. Cloud Computing Models

Cloud computing service providers offer their services on the lines of several fundamental models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a service (SaaS). Where IaaS is the most basic and each higher model abstracts from the details of the lower models.

1) **Infrastructure as a Service (IaaS):** IaaS providers offer computers, more often virtual machines and other resources as service. It provides the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. Examples of IaaS providers include: Amazon EC2, Azure Services Platform, Dyn DNS, Google Compute Engine, HP Cloud, il and etc.

2) **Platform as a Service** (**PaaS):** Cloud providers deliver a computing platform 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 acquiring and managing the underlying hardware /software layers. In PaaS, one can make applications and software's on other's database. Thus, it gives us the platform to create, edit, run and manage the application programs we want. All the development tools are provided. Some of examples of PAAS include: AWS Elastic Beanstalk, Cloud Foundry, Heroku, Force.com, EngineYard etc.

3) **Software as a Service (SaaS):** SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.

4) **Network as a Service (NaaS):** It is a category of cloud services where the capability provided to the cloud service user is to use network/transport connecting services. NaaS involves optimization of resource allocation by considering network and computing resources as a whole. Some of the examples are: Virtual Private Network, Mobile Network Virtualization etc.

5) **Communication as a Service (CaaS):** CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vender. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VolP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.

8.8. Characteristics of Cloud Computing

Cloud computing, typically entails few very important characteristics apart from the popular essentials of the computing paradigms. Few of them are given as follows:

1) **High Scalability:** Cloud environments enable servicing of business requirements for larger audiences, through high scalability.

2) **Agility (Quickness):** The cloud works in the 'distributed mode 'environment. It shares resources among users and tasks, while improving efficiency and agility (responsiveness).

3) **High Availability and Reliability:** Availability of servers is supposed to be high and more reliable as the chances of infrastructure failure are minimal.

4) **Multi-sharing:** With the cloud working in a distributed and shared mode, multiple users and applications can work more efficiently with cost reductions by sharing common infrastructure.

5) **Services in Pay-Per-Use Mode:** SLAs between the provider and the user must be defined when offering services in pay per use mode. This may be based on the complexity of services offered. Application Programming Interfaces (APIs) may be offered to the users so they can access services on the cloud by using these APIs.

6) **Virtualization:** This technology allows servers and storage devices to increasingly share and utilize applications, by easy migration from one physical server to another.

7) **Performance:** It is monitored and consistent and loosely coupled architectures are constructed using web services as the system interface.

8) **Maintenance:** The cloud computing applications are easier, because they are not to be installed on each user's computer and can be accessed from different places.

8.9. Advantages of Cloud Computing

If cloud computing is used properly and to the extent necessary, working with data in the cloud can vastly benefit all types of businesses. Major advantages of Cloud Computing are given as follows:

1) **Cost Efficiency:** Cloud computing is probably the most cost efficient method to use, maintain and upgrade. Traditional desktop software costs companies a lot in terms of finance. Adding up the licensing fees for multiple users can prove to be very expensive for the establishment concerned. The cloud, on the other hand, is available at much cheaper rates and hence, can significantly lower the company's IT expenses. Besides, there are many one-time-payments, pay-as-you-go and other scalable options available, which make it very reasonable for the company.

2) **Almost Unlimited Storage:** Storing information in the cloud gives us almost unlimited storage capacity. Hence, one no more need to worry about running out of storage space or increasing the current storage space availability.

3) **Backup and Recovery:** Since all the data is stored in the cloud, backing it up and restoring the same is relatively much easier than storing the same on a physical device. Furthermore, most cloud service providers are usually competent enough to handle recovery of information. Hence, this makes the entire process of backup and recovery much simpler than other traditional methods of data storage.

4) **Automatic Software Integration:** In the cloud, software integration is usually something that occurs automatically. This means that we do not need to take additional efforts to customize and integrate the applications as per our preferences. This aspect usually takes care of itself. Not only that, cloud computing allows us to customize the options with great ease. Hence, one can handpick just those services and software applications that s/he thinks will best suit his/her particular enterprise.

5) **Easy Access to Information:** Once registered in the cloud, one can access the information from anywhere, where there is an Internet connection. This convenient feature lets one move beyond time zone and geographic location issues.

6) **Quick Deployment:** Lastly and most importantly, cloud computing gives us the advantage of quick deployment. Once we opt for this method of functioning, the entire system can be fully functional in a matter of a few minutes. Of course, the amount of time taken here will depend on the exact kind of technology that we need for your business.

8.10. Challenges relating to Cloud Computing

In spite of its many benefits, as mentioned above, cloud computing also has certain challenges. Businesses, especially smaller ones, need to be aware of the same before adapting this technology. Major challenges are shown in Fig. 8.2.6 and discussed as follows:

1) **Confidentiality:** Prevention of the unauthorized disclosure of the data is referred as Confidentiality. Normally, Cloud works on public networks; therefore, there is a requirement to keep the data confidential the unauthorized entities. With the use of encryption and physical isolation, data can be kept secret. The basic approaches to attain confidentiality are the encrypting the data before placing it in a Cloud with the use of TC3 (Total Claim Capture & Control).

2) **Integrity:** Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are

some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.

3) **Availability:** Availability refers to the prevention of unauthorized withholding of data and it ensures the data backup through Business Planning Continuity Planning (BCP) and Disaster Recovery Planning (DRP). In addition, Availability also ensures that they meet the organization's continuity and contingency planning requirements. Availability can be affected temporarily or permanently, and a loss can be partial or complete from Temporary breakdowns, sustained and Permanent Outages, Denial of Service (DoS) attacks, equipment failure, and natural calamities are all threats to availability. One of the major Cloud service provider, AWS had a breakdown for several hours, which lead to data loss and access issues with multiple Web 2.0 services.

4) **Governance:** Due to the lack of control over the employees and services, it creates problems relating to design, implementation, testing and deployment. So, there is a need of governance model, which controls the standards, procedures and policies of the organization. The organization gains computational resources as capital expenditures. These actions should be looked by the organization under governance through legal regulation, policies, privacy and security. Auditing and risk management programs are some way to verify the policy, which can shift the risk landscape.

5) **Trust:** Trust is an important issue in Cloud. Various clients' oriented studies reveal that Cloud has still failed to build trust between the client and service provider. Trust ensures that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the Cloud provider, and their performance over time.

6) **Legal Issues and Compliance:** There are various requirements relating to legal, privacy and data security laws that need to be studied in Cloud system. One of the major troubles with laws is that they vary from place to place, and users have no assurance of where the data is located physically. An approach to monitor and compliance that helps to prepare Cloud Service Provider (CSP) and users to address emerging requirements and the evolution of Cloud models. To achieve efficiency, risk management, and compliance, CSPs need to implement an internal control monitoring function coupled with external audit process. To increase the comfort of Cloud activities, Cloud user define control requirements, internal control monitoring processes, examine applicable external audit reports, and accomplish their responsibilities as CSP users. It is the responsibility of the cloud suppliers that they are protecting the data and supplying to the customer in a very secure and legal way.

7) **Privacy:** Privacy is also considered as one of the important issues in Cloud. The privacy issues are embedded in each phase of the Cloud design. It should include both the legal compliance and trusting maturity. The Cloud should be designed in such a way that it decreases the privacy risk.

8) **Audit:** Auditing is type of checking that 'what is happening in the Cloud environment'. It is an additional layer before the virtualized application environment, which is being hosted on the virtual machine to watch 'what is happening in the system'. Its security is stronger than the one built in software and application. But, still it consumes more time, insistent across customers, pricy and motivational debilitate for everyone. The context of use of Cloud, time consuming audits seriously detains a key gain of Cloud agility.

9) **Data Stealing:** In a Cloud, data stored anywhere is accessible in public form and private form by anyone at any time. In such cases, an issue arises as data stealing. Some of the Cloud providers do not use their own server, instead. They use server/s from other service providers. In that case, there is a probability that the data is less secure and is more prone to the loss from external server. If the external server is shut down due to any legal problem, financial crisis,

natural disaster, and fire creates loss for the user. In that case, data protection is an important mechanism to secure the data. Back up policies such as Continuous Data Protection (CDP) should be implemented in order to avoid issues with data recovery in case of a sudden attack.

10) **Architecture:** In the architecture of Cloud computing models, there should be a control over the security and privacy of the system. The architecture of the Cloud is based on a specific service model. Its reliable and scalable infrastructure is dependent on the design and implementation to support the overall framework.

11) **Identity Management and Access control:** The key critical success factor for Cloud providers is to have a robust federated identity management architecture and strategy internal in the organization. Using Cloud-based "Identity as a Service" providers may be a useful tool for outsourcing some identity management capabilities and facilitating federated identity management with Cloud providers. One recurring issue is that the organizational identification and authentication framework may not naturally extend into a public Cloud and extending or changing the existing framework to support Cloud services may prove difficult. Identity Management and Access control provides a secure authentication and authorization to an organization. The identity management provides a trust and shares the digital attributes between the Cloud provider and organization ensuring the protection against attackers.

12) **Incident Response:** It ensures to meet the requirements of the organization during an incident. It ensures that the Cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Affected networks measures, determined systems, and applications, exposed intrusion vector helps to understand an incident response and the activities carried out must be re-modeled.

13) **Software Isolation:** Software isolation is to understand virtualization and other logical isolation techniques that the Cloud provider employs in its multi-tenant software architecture, and evaluate the risks required for the organization.

14) **Application Security:** Security issues relating to application security still apply when applications move to a cloud platform. To prevent Cloud computing, service provider should have the complete access to the server with all rights for the purpose of monitoring and maintenance of server. Infected applications need to be monitored and recovered by the Cloud security drivers.

8.11. Mobile Computing

It refers to the technology that allows transmission of data via a computer without having to be connected to a fixed physical link. Mobile voice communication is widely established throughout the world and has had a very rapid increase in the number of subscribers to the various cellular networks over the last few years. An extension of this technology is the ability to send and receive data across these cellular networks. This is the fundamental principle of mobile computing. Mobile data communication has become a very important and rapidly evolving technology as it allows users to transmit data from remote locations to other remote or fixed locations. This proves to be the solution of the biggest problem of business people on the move

8.12. Mobile Computing Services

The ability to share information across a wireless platform is becoming more vital to the today's business communication needs. Various companies design and develop several wireless applications and solutions for Blackberry, iPhone, Google Android G1, iPad, Windows Mobile, Symbian, Brew devices, PDA, Palm & Pocket PC. Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

8.13. Mobile Computing Benefits

In general, the mobile computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency, and improves management effectiveness. But, more specifically, it leads to a range of tangible benefits, including the following:

1) It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.

2) It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.

3) It facilitates access to corporate services and information at any time, from anywhere.

4) It provides remote access to the corporate Knowledgebase at the job location.

5) It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

8.14. BYOD

BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops, challenging the long-standing policy of working on company-owned devices. Renowned research organization 'Gartner' has predicted that by 2014, 90% of organizations will support corporate applications on personal devices. Though it has led to an increase in employees satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

8.15. Emerging BYOD Threats

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises.

Overall, these risks can be classified into four areas as outlined below:

1. **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

2. **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.

3. **Application Risks:** It is normally exemplified and hidden in **'**Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.

4. **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

5. **Mobile Computing and BYOD:** Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure. These services will focus on the issues and opportunities surrounding the new way to communicate and consume computing services. Mobile computing is not just PCs on the move. Mobile devices such as smart phones, tablets, and the iPod Touch, the last PDA standing are a radically different kind of devices, designed from the ground up as end points of data networks both internal corporate networks and the Internet rather than primarily as stand-alone devices. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life. Where laptops has a three hour battery life, the tablet and smartphone regularly run 12 hours or more between charging and serve as windows into the Cloud.

8.16. Social Media

Social networks are comprised of the most intelligent components- human beings. Being so, any activity involved with the social networks, be it participation, management, or optimization becomes extremely complicated and context based. Due to the various facets of the human species, we can have multiple types of social networks in all the fields and areas.

A social network is usually created by a group of individuals, who have a set of common interests and objectives. There are usually a set of network formulators followed by a broadcast to achieve the network membership. This happens both in public and private groups depending upon the confidentiality of the network. After the minimum numbers are met, the network starts its basic operations and goes out to achieve its goal. Success of a social network mainly depends on contribution, interest and motivation of its members along with technology backbone or platform support that makes the life easier to communicate and exchange information to fulfill a particular communication need.

8.17. Web 2.0

Web 2.0 is the term given to describe a second generation of the World Wide Web that is focused on the ability for people to collaborate and share information online. Web 2.0 basically refers to the transition from static HTML Web pages to a more dynamic Web that is more organized and is based on serving Web applications to users. Other improved functionality of Web 2.0 includes open communication with an emphasis on Web-based communities of users, and more open sharing of information. Over the time, Web 2.0 has been used more as a marketing term than a Computer Science based term. Blogs, wikis, and Web services are all seen as components of Web 2.0The main agenda of Web 2.0 is to connect people in numerous new ways and utilize their collective strengths, in a collaborative manner. In this regard, many new concepts have been created such as Blogging, Social Networking, Communities, Mashups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

CHAPTER-8
EMERGING TECHNOLOGIES

8.18. Components of Web 2.0 for Social Networks

In today's environment, computer literacy is at its peak and tools that are aided through the computerization age are most effective in keeping alive a concept as complicated as Social Networks. Major components that have been considered in Web 2.0 include the following:

1) **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking.

2) **Blogging:** Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.

3) **Wikis:** A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.

4) **Folksonomy:** Web 2.0 being a people-centric technology has introduced the feature of Folksonomy where users can tag their content online and this enables others to easily find and view other content.

5) **File Sharing/Podcasting:** This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.

6) **Mashups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

8.19. Types and Behaviour of Social Networks

The nature of social networks makes its variety. We have various types of social networks based on needs and goals. Compartmentalizing social networks is quite a challenging activity. Social networks exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas. Such huge variations make the reach of social networks grow to all sectors of the society. Keeping these in mind, the main categories identified are given below:

1) **Social Contact Networks:** These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today. They have all components of Web 2.0 like blogging, tagging, wikis, and forums. Examples of these include Orkut, Facebook and Twitter.

2) **Study Circles:** These are social networks dedicated for students, where they can have areas dedicated to student study topics, placement related queries and advanced research opportunity gathering. These have components like blogging and file sharing. Examples of these include, Fledge Wing and College Tonight.

3) **Social Networks for Specialist Groups:** These types of social networks are specifically designed for core field workers like doctors, scientists, engineers, members of the corporate industries. A very good example for this type of network is LinkedIn.

4) **Networks for Fine Arts:** These types of social networks are dedicated to people linked with music, painting and related arts and have lots of useful networking information for all aspiring people of the same line.

5) **Police and Military Networks:** These types of networks, though not on a public domain, operate much like social networks on a private domain due to the confidentiality of information.

6) **Sporting Networks:** These types of social networks are dedicated to people of the sporting fraternity and have a gamut of information related to this field. Examples of these include Athlinks.

7) **Mixed Networks:** There are a number of social networks that have a subscription of people from all the above groups and is a heterogeneous social network serving multiple types of social collaboration.

8) **Social Networks for the 'inventors':** These are the social networks for the people who have invented the concept of social networks, the very developers and architects that have developed the social networks. Examples include Technical Forums and Mashup centres.

9) **Shopping and Utility Service Networks:** The present world of huge consumerism has triggered people to invest in social networks, which will try to analyze the social behaviour and send related information for the same to respective marts and stores.

10) **Others:** Apart from the networks outlined above, there are multiple other social networks, which serve huge number of the internet population in multiple ways. Some of these networks die out very fast due to lack of constructive sustenance thoughts while others finally migrate to a more specialist network.

8.20. Life Cycle of Social Networks

The concept of social networks and the components of Web 2.0, which are significant for social networks have been outlined above. Next, we will see how Web 2.0 gets linked with the entire life cycle of a social network. For any social network, there are a number of steps in its life cycle. In each of the life cycle step of an online social network, Web 2.0 concepts have a great influence, as depicted in the Fig. 8.5.3. For all the steps in the life cycle, Web 2.0 provides tools and concepts, which are not only cost effective but very easy to implement. Often, online networks have a tendency to die out very fast due to lack of proper tools to communicate. Web 2.0 provides excellent communication mechanism concepts like Blogging and individual email filtering to keep everyone in the network involved in the day to day activities of the network.

8.21. Impact of Social Networks Using Web 2.0

Various implementations of social networks using Web 2.0 have already had a profound effect on society as a whole. One of the most important groups of people - the medical community already has reaped significant benefits from the technology and is translating the same towards the betterment of public life. According to a survey conducted by a website, almost "89% of physicians use at least one Web 2.0 tool in their medical practice" along with some other impressive figures that prove how Web 2.0 has been helping in the day-to-day activities. There are numerous reports detailing how doctors are connecting using Web 2.0 for increasing their knowledgebase. Social networks built on Web 2.0 concepts has become so cost affordable and easy to use that more and more people are migrating to this wave. This has also helped NGO's and other social service organizations to create meaningful social networks to reach out to people in a much more society. structured manner and in turn benefit the needy and deprived sector of the Society.

8.22. Future Scope of Web 2.0 in Social Networks

There is a lot of contribution that Web 2.0 has already made for social networks as well as other areas. However, the reach for the technology has not been complete and there are still a number of areas that need improvements so that the true power of the technology integrated with social networks can be truly felt. A majority of social networks still operate in an offline and unstructured manner and if proper education on Web 2.0 can be imparted, then a greater number of such networks will come under the wing of social networks Areas like space exploration, scientific experimentation, social sciences along with the area of collaborative research through social networks are something that Web 2.0 practitioners can actively contribute. The social impact that the technology is making via social networks is also making aware of the power and flexibility and is making Web 2.0 an integral part of social networks throughout the world. The future of Web 2.0 itself is something, which will

be providing much more exciting features for social networks. As time progresses, the technology is becoming more secure, robust, transparent and much more user-oriented. The concept of semantic Web is being crystallized, which will aid the growth of social networks even more. New features like online video conferencing instead of scrap messages/blogs and Object Oriented Programming will also help in introducing new features within the social network

8.23. Benefits and Challenges for Social Networks using Web 2.0

Web 2.0 has provided a number of benefits to social networks. It provides a platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time. Concepts of Web 2.0 like blogging are some things that people do on a day-to-day basis and no new knowledge skills are required. Web 2.0 techniques are very people centric activities and thus, adaptation is very fast. People are coming much closer to another and all social and geographical boundaries are being reduced at lightning speed, which is one of the biggest sustenance factors for any social network. Using Web 2.0 also increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network.

There are a number of challenges that are faced within the implementation of social networks using Web 2.0 concepts. One of the major aspects is data security and privacy and in such public domains, there is a huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such aspects. Privacy of individual users also arises and can create a huge problem if malicious users somehow manage to perpetuate the social networks. This is more important for public utility networks like doctors and police. A majority of the social networks are offline, and for bringing these under the purview of online social networks, a lot of education and advertising needs to be done, which itself becomes a cost burden, when the people involved are not computer literate. This becomes more viable in the areas of the world that are developing and do not have the basic amenities. The fact is that these areas are the ones that can benefit the most using social networks in an online mode and a huge amount of effort would be needed to help them using the technologies.

Web 2.0 has introduced a number of powerful features that social networks are utilizing. These have provided significant advances, which can be seen by the worldwide acceptance of networking sites with these technologies. In spite of all challenges, the worldwide acceptance of social networks and its implementation using Web 2.0 is here to stay and flourish. It is up to us to participate in this movement and continue to contribute towards the betterment of the technology and concept for more contribution to the society as a whole.

8.23. 8.6 Green IT

Green IT refers to the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle.

Green computing is the environmentally responsible use of computers and related resources. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste). One of the earliest initiatives toward green computing in the United States was the voluntary labeling program known as Energy Star. It was conceived by the Environmental Protection Agency (EPA) in 1992 to promote energy efficiency in hardware of all kinds. The Energy Star label became a common sight, especially in notebook computers and displays. Similar programs have been adopted in Europe and Asia.

Government regulation, however well-intentioned, is only part of an overall green computing philosophy. The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following:

1. Power-down the CPU and all peripherals during extended periods of inactivity.
2. Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times.
3. Power-up and power-down energy-intensive peripherals such as laser printers according to need.
4. Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors.
5. Use notebook computers rather than desktop computers whenever possible.
6. Use the power-management features to turn off hard drives and displays after several minutes of inactivity.
7. Minimize the use of paper and properly recycle waste paper.
8. Dispose of e-waste according to central, state and local regulations.
9. Employ alternative energy sources for computing workstations, servers, networks and data centres.

8.24. 8.6.1 Green IT Best Practices

1. From the experience of practicing professionals, there are a range of well identified best-practices. A few of those for assurance purposes are listed as follows:
2. Involving stakeholders on campus yields policies and green IT initiatives more likely to be embraced by the campus community.
3. Partnering takes advantage of existing efforts and ensures wider reach and more effective use of limited resources.
4. Guidelines for using the best practices simplify adaption of green IT by campus users and encourage them to consider green computing practices the norm.
5. On-going communication about and campus commitment to green IT best practices to produce notable results.