INTRODUCTION

Cloud computing is Internet-based Computing, whereby shared servers provide resources, software, and data to Computer and other devices on demand, as with the Cloud computing is a natural evolution of the widespread adoption of Virtualization, service-oriented and utility computing. Cloud allows access to services without user technical knowledge or control of supporting infrastructure. This is a collection/group of integrated and networked hardware, software and Internet infrastructure (called a platform). The platform provides on demand services, that are always on, anywhere, anytime and any place. These platforms hide the complexity and details of the underlying infrastructure from users and applications by providing very simple graphical interface or API (Applications Programming Interface).

Any web-based application or service offered via cloud computing is called a cloud service. Cloud services can include anything from calendar and contact applications to word processing and presentations. Almost all large computing companies today, from Google to Amazon to Microsoft, are developing various types of cloud services. Cloud services and storage are accessible from anywhere in the world over an Internet connection. Cloud computing is an umbrella term used to refer to Internet based development and services. A cloud client consists of computer hardware and/or computer software that relies on cloud computing for application delivery.

The cloud is a large group of interconnected computers. These computers can be personal computers or network servers; they can be public or private. For example, Google hosts a cloud that consists of both smallish PCs and larger servers. Google’s cloud is a private one (that is,
Google owns it) that is publicly accessible (by Google’s users). This cloud of computers extends beyond a single company or enterprise. The applications and data served by the cloud are available to broad group of users, cross-enterprise and cross-platform. Access is via the Internet. Any authorized user can access these docs and apps from any computer.

A **Virtual Private Network** is the extension of a private network that encompasses links across shared or public networks such as the Internet. A VPN enables us to send data between two computers across a shared or public inter network in a manner that emulates the properties of a point-to-point private link. In essence, it makes the remote computer virtually part of the private network by making an encrypted tunnel through the public Internet. The act of configuring and creating a VPN is known as virtual private networking.

To ensure the privacy and integrity of data as it traverses the Internet, encryption, authentication, and authorization technologies are required as well. The same requirements apply in the case of sensitive data traversing an organization’s inter network.

**Tunneling** is a method of using an intermediate network infrastructure to transfer data for one network over another network while maintaining privacy and control over the original data. The data to be transferred (the payload) can be the frames (or packets) of another protocol. Instead of sending a frame as the originating node produces it, the tunneling protocol encapsulates the frame in an additional header. The additional header provides routing information so that the encapsulated payload can traverse the intermediate network. The encapsulated packets are then routed between tunnel endpoints over the inter network. The logical path through which the encapsulated packets travel through the inter network is known as a *tunnel*. Once the
encapsulated frames reach their destination on the inter network, the frame is decapsulated and forwarded to its final destination.

Tunneling includes this entire process (encapsulation, transmission, and decapsulation of packets).

Tunneling technologies have been in existence for some time, such as SNA tunneling over IP inter networks. When Systems Network Architecture (SNA) traffic is sent across an organization’s Internet Protocol (IP) inter network, the SNA frame is encapsulated in a User Datagram Protocol (UDP) message and IP header. New tunneling technologies have been introduced in recent years. Newer technologies— which are PPTP, L2TP and IPsec TM. For a tunnel to be established, both the tunnel client and the tunnel server must be using the same tunneling protocol. Tunneling technology can be based on either a Layer 2 or a Layer 3 tunneling protocol.

Security for Windows VPN connections is a combination of basic elements that are required (authentication, authorization, encryption, and packet filtering) and advanced features that provide additional protection (such as certificate based authentication, network access quarantine control, and remote access account lockout).