# Chapter 1: Introduction

In recent years with the bloom of the field of solid state, lighting leads to the replacement of florescent lamps by Light Emitting Diodes (LEDs) which further motivates the usage of Visible Light for communication (VLC). Exponential growth in LED usage which has been experienced, may have caused opening up researchers' eye towards exploring methods to use already existing, widely available LED infrastructure to use as the communication medium which finally resulted in using the visual light spectrum for data transfer [1]. Visible Light Communication or VLC is a novel communication method that most researches have put faith on to become the communication technology of the next generation. It uses Light Emitting Diodes’ (LED) ability to switch into different intensity levels at a fast rate to transfer data [1-2]. LEDs will be the future of modern lighting system as they enjoy many advantages over conventional lighting devices. LED is known to be an efficient illumination source. The VLC technology in addition to illumination is also used to send information using the same light signal. In literal terms, any information that can be sent using a light signal that can be visible to the human eye is considered to be VLC but most importantly light should be visible to humans but not the data we transfer through it.

The opportunity to send data usefully in this manner has largely arisen and under research because of the widespread use of LED light bulbs. We can switch LEDs at very high speed that was not possible with older light sources such as fluorescent and incandescent lamps. The adaptation of LED light bulbs during the last few years has created a massive opportunity for VLC. The problem of congestion of the radio spectrum utilized by Wi-Fi is also helping to the improvement of VLC. The Radio Frequency (RF) communication suffers from high latency and interference issues and also it requires a separate setup for transmission and reception of RF waves. Overcoming the above mentioned issues VLC can be used as a preferred communication technique because of its high bandwidth and immunity to interference from electromagnetic sources.

The world has moved to use wireless technology decades ago replacing the wired technologies available for Internet connectivity. Wi-Fi is the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections with devices based on the IEEE 802.11 standards [3]. Wi-Fi is the widely used wireless technology to connect with the global Internet. In Wi-Fi when an RF current is supplied to an antenna, an electromagnetic field is created that is able to propagate through space. The main component of a wireless network is a device known as an Access Point (AP). The primary job of an access point is to broadcast a wireless signal that can be detected by computers and "tune" into. That is the main problem that we have identified in the available Wi-Fi technology. When establishing a Wi-Fi connection there is a 3-step process to get connect to an AP or wireless router where authentication happens. Same RF is used to share the secret key in the existing Wi-Fi technology. Thus, if the Wi-Fi has not given an open access, users, who are connecting need to provide user name and password to authenticate at least once. The problem here is anyone within the range of the Wi-Fi can get access once they have authenticated and if not forget.

Through this paper, we are proposing a novel protocol for location dependent Internet connectivity using VLC. This authentication protocol mainly depends on VLC to share the secret key for user authentication and once authenticated, available Wi-Fi technology can be used for data transfer. Our main target is to provide location-based Internet access which will ultimately result in more restricted access to Wi-Fi where more sensitive and confidential data transfer is required. The available Wi-Fi access points use password authentication but anyone within the range of the access point who has the password can get access. However, using this novel protocol, we can restrict the access to a single indoor location or a room. The proposed protocol uses the existing infrastructure to achieve its objective.