1. INTRODUCTION

The popularity of online social network is increasing tremendously day by day. The user base of facebook alone is more than 850 millions. Over the past several years, several Online Social Network (OSN) sites like myspace, facebook, twitter, LinkedIn have been arisen to provide their users social interactions with friends, colleagues, family as well as strangers. Information provided by user which is well known as a profile contains photo, First name, Last name, Mobile number, Home town, Qualification, the organisation where he works etc. Some of these fields are mandatory and remaining are optional and varies from one OSN to the other. To attract more and more friends or to let others to find easily the users try to provide the maximum information in the profile.

Apart from the above fields the OSN provides flexibility to the user to add information about his school, college, other interests, activities and so many other things. By providing such information on the OSN it is easier to get more connections of people having same school, college as well as same interest, activities and so on. By revealing such maximum information the user is not only attracting his friends but strangers also. It is found that on facebook on an average every user is having 150 contacts/friends.

Other than the profile of user lot many other things are present on his webpage. The wall contains the posts written by his friends which sometimes may contain sensitive information. The webpage also contains photos uploaded/published by the user. It also contains the list of friends of the user by using which it is possible to access their web pages also. The messages section in Facebook contains short messages which are send to the user by his friends.

Online Social Network is the easiest way to be connected with friends, colleagues as well as establish new contacts with the strangers. OSN enable people to connect with their friends as
well as share information about their personal life. OSNs are mainly used for keeping in touch with friends, forming new contacts, as well as search for someone else on the OSN and establish contact with him by sending a friend request. Such contacts are used to share some information with each other as well as broadcast the information through a group.

Due to the availability of more number of OSNs some of the users are having their account on more than one OSN so that they can remain in touch with their friends in that OSN also. While creating such profiles or accounts most of the users doesn’t go through the privacy policy of each such OSN and provide the information. In such cases there is high risk of information leakage.

By making some sensitive/ private fields accessible to everyone there are chances of personal information leakage. The personal information privacy oversight leads to the personal information leakage. Malicious users take advantage of these profiles to collect other’s private / secret information which leads to personal information leakage which is a threat to the privacy of user.

In addition or as an alternative to the deployment of privacy preserving techniques, one may consider methods of detecting or discouraging leaks of sensitive information. It is observed that the OSN users are not much serious about the privacy of their profile in this digital world of OSN. The privacy may be at risk in social networking sites, as maximum information is willingly provided. Different factors are likely to drive information revelation in Online Social Network. Due to the following inbuilt properties of the OSN they are more prone to privacy and security threats:-

- Very large and distributed user base.
Group of users based on particular attribute like organization where he work, area of interest etc.

The Online Social Networks allows user to post their own applications on the OSN which will be accessible by all others, such apps may be harmful.

These features are used so many times in the past to perform attack on the OSN.

There are some serious privacy problems that need to be resolved in existing OSN. There has to be a mechanism to protect user-provided data in the profile as well as user-generated data by the OSN providers. Similarly a fully flexible and dynamic access control mechanism should exist to protect private data against attackers and unauthorized users. The access control system should be efficient in managing the privacy policies of OSN users. These users are having frequent communication with each other. So the adversaries find the OSN as a soft target to attack easily and spread it like a wildfire to large number of users in no time. Now a days such security threats are coming in picture and are reported by the Online Social Networks, users as well as researchers.

It is observed that so many OSN users simply accept friend request or send friend request though he does not know the person in real life or he may not be the same person as assumed by the user sending/accepting friend request. Such habits will lead to privacy breaches because whatever data/fields are accessible to the friends of profile owner will be used by such people and the private/sensitive information can be misused. Even such simplest form of privacy breach can lead to havoc as 75,000 out of 2,50,000 facebook users accepted the friendship request which was actually generated by using automated script. This clearly indicate that the particular user can now get access to more than 75,000 user’s data on facebook which can be utilized for any of the purpose.
In this scenario the user awareness is important to protect privacy of the information provided by the user. Similarly the OSN providers must take due care of the privacy and security of the user data. So security framework for Online Social Network is necessary which will try to reduce such kind of threats and attacks on the Online Social Network.

As the OSN follow the client-server architecture all the data given by the user in the profile will remain with the server so no one can predict that how secure is the data. So to overcome such threats it is necessary to design a security framework for Online Social Network, which will reduce the security threat to the Online Social network.