Social Network Site (SNS) has become popular due to its social nature. SNS make the users to create and improve their online contacts. Normally, basic structure of SNS includes the following features, namely, Profile, Friend, Forums and Groups.

Profile helps the user to represent them to the outside world. By using friends, user’s contacts get increased. Forum helps the user to carry over discussion on a specific theme. Here forums can be restricted to specific user set based on their age, interest or other characteristics. Groups create an avenue for multicast communication among its members.

Since SNS is constructed as user centric, it is very difficult to protect the user’s personal information. No one can assure the trust level of the users. Thus, the environment is vulnerable to identity and data theft. The major weakness in the internet (applicable to SNS as well) is its lackness of well defined reliable authentication mechanism with high usability.

Authentication ensures the identity of an entity. It assures the identity as it is claimed. Authentication process comprises of two phases,
i. Submission of credentials and

ii. Verification

The credentials may be, something user knows, something user have, and something they are. The best example for option 1 is password, smart card for second option and biometric for third option.

While it is decided to impose a security in a system, it is necessary to investigate the system as well as the user. Since, the inclusion of security should not be a hindrance to its usability. Hence, security akin to usability needs to be taken together for any investigation on SNS. Usability in SNS therefore depends on the nature of users using a particular SNS.

Bearing in mind this important criterion, present research focuses on a parametric study in existing/enhanced security mechanisms of selected but proven protocols, considering in parallel the usability of specific users of SNS. The research attempts to propose a reliable authentication model for restricted forums of SNS.

Three parameters are considered in the research to identify the feasible authentication mechanism suitable for SNS. The parameters are, usability, security and robustness. Empirical weightages have been derived for these parameters by Delphi method and feedback from a set of respondents.
The authentication mechanism delimited to the present research is listed below.

1. Password based authentication mechanism
2. Token based authentication mechanism
3. Biometric based authentication mechanism
4. Signature based authentication mechanism and
5. Group key based authentication mechanism

Literature survey was done over the existing methods/algorithms in each category. Empirical weightage values for the mechanism based on the security parameters is derived for its various identified levels. Based on the social nature, with respect to the weightages on the three parameters, the optimum valued security mechanism has been considered for the design of the proposed model.

Two way password-personalised questioned based authentication model

This security model aims to provide authentication for the users while they are updating their profile. Normally password based authentication is popular for this case. But, by considering the demerits of password based mechanism, as well as to increase the robustness of the model, personalized questions are considered as a second factor. The security requirement is not being fulfilled with this second factor alone, hence keys are generated from these factors and some cryptographic procedures are executed to strengthen the security level.
Three way signature based authentication model

In this security model, it is tried to secure the messages exchanged in the restricted user forums. Since the forum is restricted, the messages need to be exchanged in a secured way. Thus, a reliable signature based authentication model is proposed to verify the user and to generate the keys, which are used as a session key. Here Centralized Agency (CA) plays a vital role to generate the keys. The robustness and the reliability of the model is ensured by the signature generated by the user.

Distributed contributory authentication model

Secret groups of SNS provide an efficient way to establish communication among the higher level authorities of an industry/organization. In the proposal, it is tried to generate the group key using Chinese Remainder Theorem (CRT). Here, the members have to contribute their information to generate keys during every member join process. The keys can be calculated in a distributed way after a member leaves the group. The robustness of the key is ensured by the user’s secret code which can be updated for every join operation.

The validation is carried out in two phases on all the above three models. The first phase consists of technical validation and the second one is social validation through social surveys. A sample of South Indian respondents have been considered for the validation purpose.