**SYSTEM ANALYSIS**

**EXISTING SYSTEM:**

* So far, the research community has paid little attention to OSN apps specifically. Most research related to spam and malware on Facebook has focused on detecting malicious posts and social spam campaigns.
* Gao *et al.* analyzed posts on the walls of 3.5 million Facebook users and showed that 10% of links posted on Facebook walls are spam. They also presented techniques to identify compromised accounts and spam campaigns.
* Yang *et al.* and Benevenuto *et al.* developed techniques to identify accounts of spammers on Twitter. Others have proposed a honey-pot-based approach to detect spam accounts on OSNs.
* Yardi *et al.* analyzed behavioral patterns among spam accounts in Twitter.
* Chia *et al.*investigate risk signaling on the privacy intrusiveness of Facebook apps and conclude that current forms of community ratings are not reliable indicators of the privacy risks associated with an app.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Existing system works concentrated only on classifying individual URLs or posts as spam, but not focused on identifying malicious applications that are the main source of spam on Facebook.
* Existing system works focused on accounts created by spammers instead of malicious application.
* Existing system provided only a high-level overview about threats to the Facebook graph and do not provide any analysis of the system.

**PROPOSED SYSTEM:**

* In this paper, we develop FRAppE, a suite of efficient classification techniques for identifying whether an app is malicious or not. To build FRAppE, we use data from MyPage- Keeper, a security app in Facebook.
* We find that malicious applications significantly differ from benign applications with respect to two classes of features: On-Demand Features and Aggregation-Based Features.
* We present two variants of our malicious app classifier— FRAppE Lite and FRAppE.
* FRAppE Lite is a lightweight version that makes use of only the application features available on demand. Given a specific app ID, FRAppE Lite crawls the on-demand features for that application and evaluates the application based on these features in real time.
* FRAppE—a malicious app detector that utilizes our aggregation-based features in addition to the on-demand features.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The proposed work is arguably the first comprehensive study focusing on malicious Facebook apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection approach.
* Several features used by FRAppE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are robust to the evolution of hackers.