**SYSTEM ANALYSIS**

**Existing System:**

Whenever a user types in her password in a bank’s signin box, the keylogger intercepts the password. The threat of such keyloggers is pervasive and can be present both in personal computers and public kiosks; there are always cases where it is necessary to perform financial transactions using a public computer although the biggest concern is that a user’s password is likely to be stolen in these computers. Even worse, keyloggers, often rootkitted, are hard to detect since they will not show up in the task manager process list.

**Proposed System:**

Our approach to solving the problem is to introduce an intermediate device that bridges a human user and a terminal. Then, instead of the user directly invoking the regular authentication protocol, she invokes a more sophisticated but user-friendly protocol via the intermediate helping device. Every interaction between the user and an intermediate helping device is visualized using a Quick Response (QR) code. The goal is to keep user-experience the same as in legacy authentication methods as much as possible, while preventing keylogging attacks.