**INTRODUCTION:**

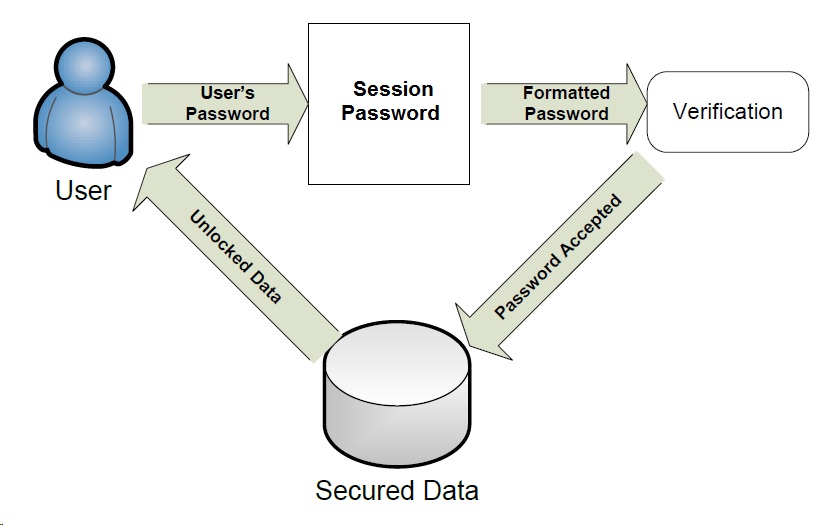
The most common method used for authentication is textual password. The vulnerabilities of this method like eves dropping, dictionary attack, social engineering and shoulder surfing are well known. Random and lengthy passwords can make the system secure. But the main problem is the difficulty of remembering those passwords. Studies have shown that users tend to pick short passwords or passwords that are easy to remember. Unfortunately, these passwords can be easily guessed or cracked. The alternative techniques are graphical passwords and biometrics. But these two techniques have their own disadvantages. Biometrics, such as finger prints, iris scan or facial recognition have been introduced but not yet widely adopted.

There are many graphical password schemes that are proposed in the last decade. But most of them suffer from shoulder surfing which is becoming quite a big problem. There are graphical passwords schemes that have been proposed which are resistant to shoulder-surfing but they have their own drawbacks like usability issues or taking more time for user to login or having tolerance levels. Personal Digital Assistants are being used by the people to store their personal and confidential information like passwords and PIN numbers. Authentication should be provided for the usage of these devices**.**

**OBJECTIVE/AIM:**

There is growing interest for Graphical passwords since they are better than Text based passwords. This project details the architecture of a graphical password system for a device. We emphasize using the system on small mobile devices.

**TECHNICAL DETAILS:**



* The user interacts with external interface module.
* The external interface module interacts with internal verification module.
* The verification module accepts or rejects the user’s password attempt and either allows or blocks access to the targeted file.

**INNOVATIVENESS AND USEFULNESS:**

A graphical password will offer increased security compared to a text password because constructing the password is limited by the number of pixels on the screen instead of the number of keys on a keyboard. A graphical password also takes advantage of the available hardware by offering a more natural task for the user than clicking letters on the on-screen keyboard.

**CURRENT STATUS OF DEVELOPMENT:**

The graphical password system is meant to replace the default text password system anywhere it would be invoked, such as at login, when installing software, when accessing restricted files, etc. Before two decades for the text password are as follows,

* Alpha-numeric passwords guidelines
  + - At least 8 characters long.
    - Should not be easy to relate to the user (e.g. last name, birth date).
    - Should not be a word that can be found in a dictionary or public dictionary.
    - Should combine upper and lower case letters and digits.
* Vulnerabilities
  + - Shoulder surfing (watching a user log on as they type their password).
    - Dictionary attacks.
    - User may forget the password if it is too long and complicated.

**COMPETITIVE ADVANTAGE:**

* Resistant to eves dropping, shoulder surfing
* Due to dynamic passwords, dictionary attack is not applicable.
* Session passwords can be used only once and every time new password is generated.
* Brute force attack is not applicable.

**Prof. O.D.Joshi Prof.O.D.Joshi Prof.S.S.Bharadwaj**

**Guide Co-ordinator HOD,CSE**