* 1. **INTRODUCTION**

Passwords are used to provide authentication in any system like a mobile device. Alphanumeric passwords are in use for user authentication. While today other methods including biometrics and smart cards are possible alternatives, passwords are likely to remain dominant for some time because of concerns about reliability, privacy, security, and ease of use of other technologies. However, in the use of passwords dilemmas often arise in the tradeoff between security and usability. The dilemma arises because passwords are expected to comply with two basic conflicting requirements:

**(1)** Passwords must be easy to recall and remember and

**(2)** Passwords should be secure, i.e., they should look random and should be hard to guess.

They should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text. Because it is difficult for humans to remember random strings, users tend to ignore requirements for secure passwords. This leads to poor password practices, including short, simple passwords that are easy to break either by a dictionary attack or personal knowledge of the password owner, use of the same password over months or years, reuse of identical or nearly identical passwords on multiple systems, and propensity to write down passwords and store them insecurely, e.g., a text file containing the users passwords stored on insecure computers or PDAs, post its notes stuck on or near the computer monitor or inside a desk drawer. In an effort to improve password security by making passwords easier to remember, graphical passwords have been proposed. In a typical graphical password scheme, a user chooses several colors present in a grid or a matrix to be his or her password. When logging in, the user must click on the password colors among a larger group of distractor colors. If the user chooses the correct colors, he or she is authenticated. User’s memory for a graphical password may be better than for an alphanumeric password. Secure alphanumeric passwords (i.e., random strings) are based on ability to recall from memory, a task that is difficult for humans. By contrast, graphical passwords are based on recognition of previously known images, a skill at which humans are proficient. However, the problem of shoulder- surfing is a recognized drawback of graphical passwords.

**AIMS AND OBJECTIVES**

1. The graphical passwords provide better security against dictionary and brute force attacks as login grid changes for every session.
2. It is very economic and very useful to user because it does not use any sophisticated devices or technology for implementation thus people implementing it can use the system even if they have minimal computer knowledge and would not have to go through any kind of training to use the system.
3. Compare two systems hybrid textual authentication scheme and color grid pattern matching.
4. Passwords must be easy to recall and remember and Passwords should be secure, i.e., they should look random and should be hard to guess.
5. The aim of the project is to implement two types of graphical password authentication techniques i.e. color grid based and pattern based.
6. The system also aims at integrating the two techniques and comparing all the schemes to determine which is a better one.