**CMAPS: A Chess-Based Multi-Facet Password Scheme for Mobile Devices**

**Alternate title:-Multi Factor Authentication Based on Game Mode**

**Aim:**

The main aim of this project is to give high secured Authentication password scheme which user can easily remember.

**Synopsis:**

The popularity of mobile devices is due to a unique set of features including ubiquitous Internet access through communication technologies such as WiFi and 4G/LTE, easy to use touch-based inputs, and numerous applications and games. In the meantime, the security of mobile devices is becoming a major concern as device users are storing sensitive data such as personal contacts and utilizing sensitive applications like banking and stock trading. Authentication, the first defense mechanism preventing unauthorized access to a mobile device, allows owners of mobile devices to unlock and use their devices. Designing an authentication scheme for mobile devices is a challenging task because the scheme should be secure, capable of generating human-memorable passwords, and usable.

**Existing Method**

A secure authentication scheme should have a large password space, i.e., a large number of possible passwords. Obviously the passwords generated by the scheme should also be easy to remember. In this paper, we separate memorability from usability to emphasize the importance of memorability. It has long been recognized that no silver bullet exists to achieve both security and memorability. Obviously with the addition of a usability requirement, the task becomes even more challenging. The alphanumeric password scheme, which has been used for decades for various computer systems, is not suitable for mobile authentication. The scheme generally requires a keyboard for quick input of alphanumeric passwords.It has long been recognized, by both security researchers and human-computer interactionresearchers that no silver bullet for authentication exists to achieve security, usability, and memorability.

**Proposed Method**

We propose a Multi-facet Password Scheme (MAPS) for mobile authentication. MAPS fuses information from multiple facets to form a password, allowing MAPS to enlarge the password space and improve memo ability by reducing memory interference, which impairs memory performance according to psychology interference theory. The information fusion in MAPS can increase usability, as fewer input gestures are required for passwords of the same security strength. Based on the idea of MAPS, we implement a Chess-based MAPS (CMAPS) for Android systems. Only two and six gestures are required for CMAPS to generate passwords with better security strength than 4-digit PINs and 8-character alphanumeric passwords, respectively. Our user studies show that CMAPS can achieve high recall rates while exceeding the security strength of standard 8-character alphanumeric passwords used for secure applications.

**Modules**

* **User Registration & OTP Verification**
* **Single Hand Gesture**
* **Multi Hand Gesture**
* **Forget Password Feature**

**User Registration & OTP Verification**

The user who is going to use the authentication scheme has to do registration. Whenever new registration is initiated the user has to enter their basic details. Once when the user enters into the system with the registered credentials the system allows the user to Gesture registering module.

**Single Hand Gesture**

When the user has to register with the gesture, they have to move finger over the touch screen without taking away the finger. The OTP verification will be done where OTP will be received to user’s registered mobile number. Once when the gesture function get over the session get completed and the new single hand gesture password will be stored in the database as encrypted.

**Multi Hand Gesture**

When the user has to register with the gesture, they have to move finger over the touch screen step by step taking away the finger multiple times. Once when the gesture function get over the session get completed and the new multi hand gesture password will be stored in the database as encrypted.

**Forget Password Feature**

When the user does not able to recognize the registered password they can opt for forget password. Once again the OTP will be received to the registered user’s mobile. When the user is authenticated the CMAPS system will allow for new password registration.

**Software Requirements**

* Windows 7 and Above
* JDK 1.7
* Tomcat 7.0
* MySql 5.0

**Hardware Requirements**

* Hard Disk : 200GB and Above
* RAM : 2GB and Above
* Processor : i3 and Above

**Technology Used**

* + - J2EE (JSP, Servlets)
    - JavaScript , HTML ,CSS ,AJAX

**Architecture**

****

User authentication

Otp verification

Check layout password reg

Single head

Multi head

Check layout

Verification

Authentication success

Authentication failed

Allows application

Verification success

