International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Password Security Using Cued Points and Cryptography

[1]Dr.M.M.Bokare, [2]Mr.A.V.Suryawanshi

Department of Computer Science

SSBES' Institute of Technology and Management, Nanded.

Abstract

The most popular security method for safeguarding digital assets is password-based authentication. However, there are a number of issues with typical text-based passwords, including phishing, dictionary attacks, brute-force attacks, and poor memorability. Graphical password methods, which take advantage of people's cognitive capacity to retain visual information, have been developed to get around these restrictions. This work introduces a secure authentication method that combines cryptographic techniques with graphical passwords based on cued points. While cryptographic techniques like hashing, salting, and encryption guarantee the safe storage and transfer of authentication data, cued points offer visual clues that enhance usability. The suggested system preserves user convenience while strengthening defense against frequent attacks. Applications, security analysis, working methodology, and system architecture are all well covered.

Keywords : Password Security, Cued Points, Graphical Passwords, Cryptography, Authentication.

I. INTRODUCTION

An essential component of information security systems is authentication. Passwords continue to be the most often used approach among the three authentication factors—something the user knows, something the user has, and something the user is—because of their affordability and ease of use. Enforcing strong text-based passwords, however, frequently results in usability problems and weak or reused passwords.

An alternative is offered by graphic password schemes, which make use of visual memory and graphics. The cued point technique, which uses visual cues to assist people select particular places on an image, is one efficient method. Cued point authentication can greatly enhance security and usability when used with cryptographic methods.

II. RELATED WORK

Graphical password authentication schemes have been investigated by a number of researchers. To address the shortcomings of text passwords, recognition-based, recall-based, and cued recall systems have been developed. Users click on one point each image in a series of photos under the well-known Cued Click Points (CCP) technique. To safeguard saved password data, cryptographic methods like secure hashing and salting are frequently employed.

III. CUED POINT–BASED PASSWORD SYSTEM

A cued point–based password system allows users to select one or more points on an image during registration. The image acts as a cue, helping users recall their password accurately.

A. Registration Phase

1. User selects an image from a predefined image set.

2. User clicks on one or more points on the image in a specific order.

3. The system records the (x, y) coordinates of the selected points.

4. Cryptographic processing is applied before storing the data.

B. Login Phase

1. The same image is displayed to the user.

2. User clicks on the previously selected points.

3. The system checks whether the clicked points fall within the tolerance region.

4. Access is granted if all points match.

IV. SYSTEM ARCHITECTURE

The proposed system architecture consists of multiple components working together to provide secure authentication.

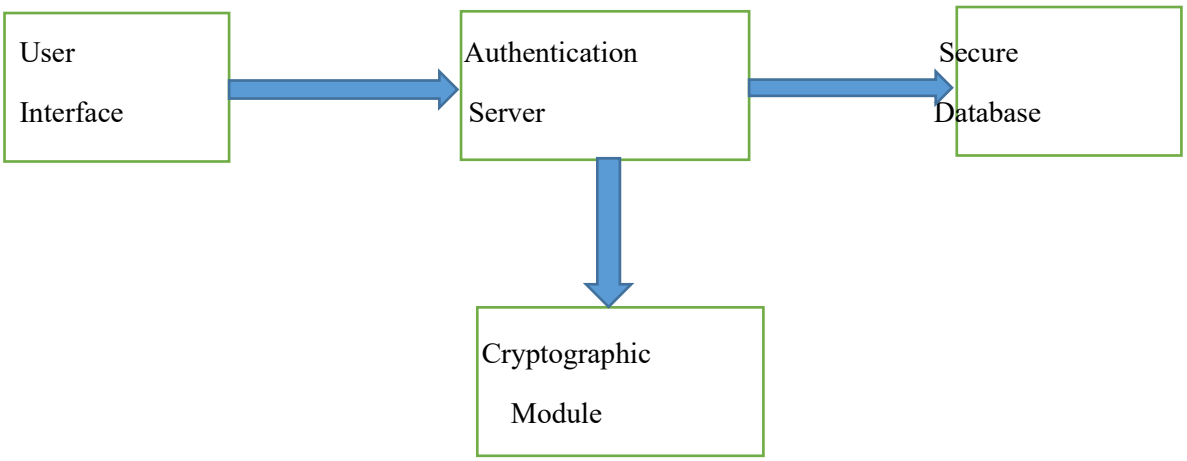

Fig. 1. System Architecture of Cued Point Authentication System

V. CRYPTOGRAPHIC INTEGRATION

Cryptography ensures that cued point data is protected against unauthorized access.

A. Hashing and Salting

The selected cued point coordinates are concatenated and hashed using secure algorithms such as SHA-256 or bcrypt. A unique salt is added to prevent rainbow table attacks.

B. Encryption

Sensitive metadata, such as image identifiers and tolerance values, is encrypted using symmetric encryption algorithms like AES.

C. Secure Communication

All communication between client and server is secured using TLS to prevent eavesdropping and man-in-the-middle attacks.

VI. WORKING METHODOLOGY

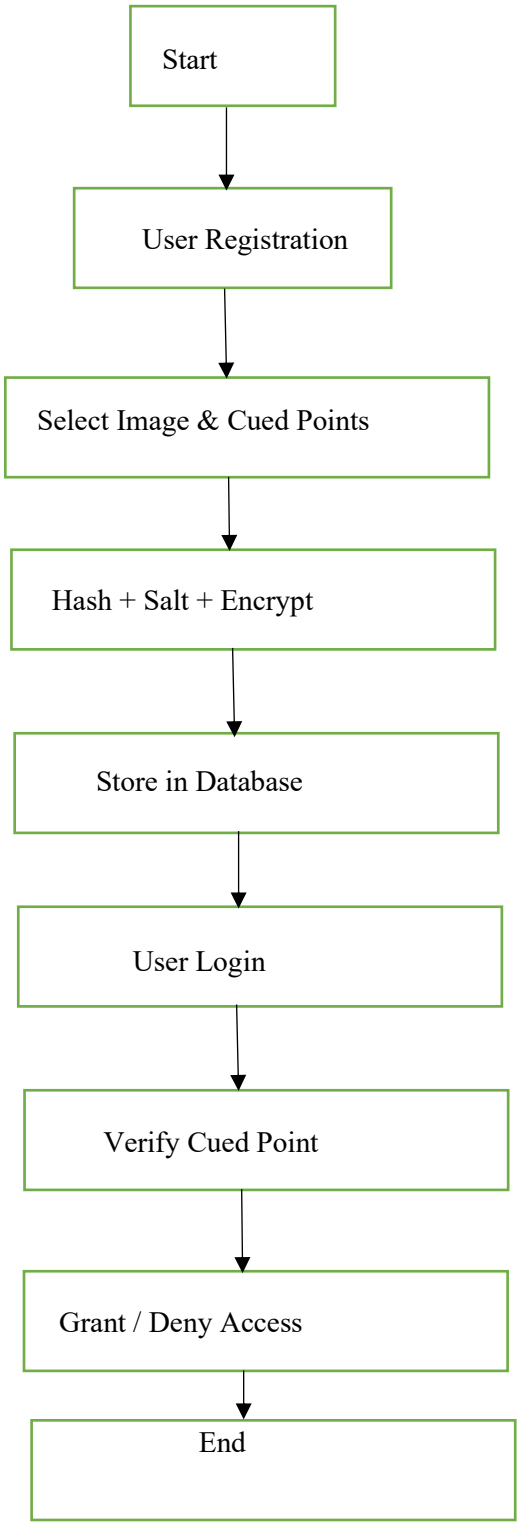

Fig. 2. Flow Diagram of Cued Point Authentication Process

VII. SECURITY ANALYSIS

A. Brute-Force Resistance

The password space is significantly larger due to the large number of possible pixel combinations.

B. Dictionary Attack Resistance

Graphical passwords are not based on predictable textual patterns.

C. Shoulder Surfing

Tolerance regions and optional dynamic images reduce observation-based attacks.

D. Database Attacks

Even if the database is compromised, hashed and salted data prevents recovery of original cued points.

VIII. ADVANTAGES AND LIMITATIONS

A. Advantages

- Improved memorability using visual cues
- Large password space
- Strong resistance to common attacks
- Enhanced user experience

B. Limitations

- Higher storage and processing overhead
- Accessibility challenges for visually impaired users

IX. APPLICATIONS

- Online banking systems
- Secure enterprise applications
- E-learning platforms
- Mobile and web authentication

X. CONCLUSION

The integration of cued point–based graphical passwords with cryptographic techniques provides a robust and user-friendly authentication mechanism. By combining visual memory with secure cryptographic storage, the proposed system enhances password security while maintaining usability. This approach shows strong potential for adoption in modern secure systems.

REFERENCES

[1] D. Davis et al., "Authentication Using Graphical Passwords," IEEE Security & Privacy, vol. 2, no. 4, pp. 38–45.

[2] W. Jansen, "Authenticating Users on Handheld Devices," NIST Report.

[3] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press.

[4] R. Gawade et al., "Cued Click Points: A Graphical Password Scheme," International Journal of Computer Applications.