Design and implementation of a secure hybrid authentication system using freehand drawing and typed password

Enhancing User Authentication Through Multi-Modal Security Mechanisms

V. Iswarya[1], B. Ruthra[2], A. Pannerselvam[3]

[1] Final Year Student, Department of Computer Science and Engineering

[2] Final Year Student, Department of Computer Science and Engineering

[3] Final Year Student, Department of Computer Science and Engineering

SRG Engineering College, Tamil Nadu, India

Email IDs:

i2409027@gmail.com,srikumarantkm@gmail.com, selvamsr06@gmail.com

***Abstract*— This paper presents the design and implementation of a secure hybrid authentication system that integrates freehand drawing and traditional typed passwords. Conventional authentication methods, such as text-based passwords, are vulnerable to attacks including brute force, shoulder surfing, and phishing. To overcome these limitations, the proposed system introduces a dual-layer authentication mechanism combining graphical and textual inputs.**

In this system, users first create a unique freehand drawing pattern, which acts as a graphical password. This is followed by a conventional typed password, forming a hybrid authentication model. The graphical component enhances resistance to observation attacks, while the textual component adds an additional security layer. The system is implemented using user-friendly interfaces and efficient pattern recognition techniques to ensure accuracy and usability.

Experimental results demonstrate that the proposed system improves security without significantly affecting user convenience. The hybrid approach provides a balanced solution between usability and protection, making it suitable for modern secure applications.

Index Terms

Hybrid Authentication, Graphical Password, Freehand Drawing, Text-Based Password, Security, Multi-Factor Authentication

I. Introduction

With the rapid growth of digital systems, secure authentication has become a critical requirement. Traditional password-based systems are widely used but suffer from several vulnerabilities, including weak password selection and susceptibility to attacks such as brute force and phishing.

To address these challenges, graphical password techniques have been introduced, leveraging human memory's ability to recognize images and patterns more effectively than text. However, graphical systems alone may still have limitations in terms of precision and storage.

This paper proposes a hybrid authentication system that combines freehand drawing with typed passwords. By integrating both methods, the system enhances overall security while maintaining usability. The objective is to design a system that is resistant to common attacks while being intuitive for users.

III. Ease of Use

The proposed system is designed with user convenience in mind. The freehand drawing interface is simple and intuitive, allowing users to easily create and reproduce their graphical passwords. The addition of a typed password ensures familiarity, reducing the learning curve for new users.

Before implementing the system, the design and requirements were clearly defined. The development process included separating the graphical input module and the textual password module, followed by integration into a unified authentication system. Proper testing was conducted to ensure reliability and accuracy.

Abbreviations and Acronyms

MFA – Multi-Factor Authentication

GUI – Graphical User Interface

API – Application Programming Interface

Units

All measurements and system parameters used in this project follow standard SI units to maintain consistency and clarity.*)*

I. INTRODUCTION (HEADING 1)

All manuscripts must be in English. These guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts. Please follow them.

This template provides authors with most of the formatting specifications needed for preparing electronic versions of their papers. Margins, column widths, line spacing, and type styles are built-in; examples of the type styles are provided throughout this document and are identified in italic type, within parentheses, following the example. PLEASE DO NOT RE-ADJUST THESE MARGINS. Some components, such as multi-leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

Abbreviations and Acronyms (Heading 2)

The following abbreviations are used in this paper:

MFA – Multi-Factor Authentication

GUI – Graphical User Interface

API – Application Programming Interface

PIN – Personal Identification Number

AI – Artificial Intelligence

All abbreviations are defined at their first occurrence and used consistently throughout the paper.

Units

This paper follows the International System of Units (SI) for all measurements and parameters. Where necessary, additional units are provided in parentheses for clarity.

For example, system response time is measured in seconds (s), and storage requirements are measured in megabytes (MB). Care is taken to avoid mixing different unit systems to maintain consistency and prevent ambiguity.

Equations

The authentication accuracy and system performance can be expressed using the following equation:

Similarly, the error rate is calculated as:

These equations help evaluate the effectiveness of the hybrid authentication system by measuring user success rates and system reliability.

Some Common Mistakes

While preparing this paper, the following common mistakes were carefully avoided:

The word “data” is treated as plural, not singular.

Proper capitalization is maintained for technical terms and headings.

Punctuation is placed correctly with quotation marks and parentheses.

Consistent terminology is used throughout the paper (e.g., “authentication system” instead of switching terms).

Avoided informal or vague words such as “essentially” or “approximately” unless required.

Attention to these details ensures clarity, professionalism, and adherence to IEEE writing standards.

Language and Writing Guidelines

Words such as “using” are kept in lowercase in the title unless grammar requires capitalization.

Homophones like “affect” and “effect”, “principal” and “principle” are used correctly.

The prefix “non” is written without a hyphen unless necessary.

Abbreviations such as “i.e.” (that is) and “e.g.” (for example) are used appropriately.

II. ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the faculty members of the Department of Computer Science and Engineering, SRG Engineering College for their continuous guidance and support throughout the development of this project.

Special thanks are extended to our project guide for valuable suggestions and encouragement during the design and implementation of the hybrid authentication system.

REFERENCES

1. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," Pattern Recognition, vol. 38, no. 12, pp. 2270–2285, 2005.

2. R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Computing Surveys, vol. 44, no. 4, 2012.

3. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," Annual Computer Security Applications Conference, 2005.

4. W.Stallings, Cryptography and Network Security, 7th ed., Pearson, 2017.