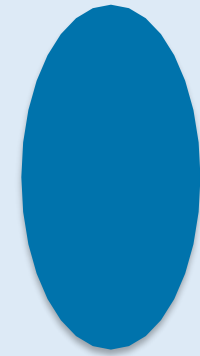


Static Keystroke Dynamic Authentication Model to Authenticate User During Password Change



Presented by

V. Sai sneha (21RP1A05B8)
S. Kavyanjali (21RP1A05A4)
P. Shruthi (21RP1A0596)
N. Himabindu (21RP1A0587)

Guided by

P. Venu Madhav

Content

- ✓ Abstract
- ✓ Introduction
- ✓ Existing System
- ✓ Disadvantages of Existing System
- ✓ Proposed System
- ✓ Advantages of Proposed System
- ✓ System Requirements
- ✓ Implementation
- ✓ Testing / Experimentation
- ✓ Results
- ✓ Future Enhancement
- ✓ Conclusion
- ✓ References

1. Abstract

Keystroke dynamics is considered as a supporting factor of authentication. Especially in the static keystroke dynamics, the user is identified by using the timing featured, which is captured while the user enters the login ID and password. To achieve this, the user profile needs to be created with timing features. However, in a scenario like a change of password where nearly no keystroke timing data is available, non-conventional features may be helpful. This article focuses on using non- conventional features such as NumLock key, Shift key, Capslock key, etc, for identifying users during a change of password. The paper also details how to capture the non-conventional features in static keystroke dynamics and build a model that can be used in the change of password.

2. Introduction

- ✓ As password based authentication has many limitations many times to strengthen the authentication, multi factor authentication is used.
- ✓ Password based authentication is the most frequently used authentication method for providing access to personal computers, online services and Internet access.
- ✓ Here we use a support factor of authentication is keystroke dynamics, which is based on behavioral characteristics of a user.
- ✓ There are two types of key stroke dynamics: Static and Continuous .In the static keystroke dynamics, the typing rhythm of a user is captured only at login time.

Keystroke Dynamic Authentication

HOME USER ADMIN REGISTER



KEYSTROKE DYNAMICS SYSTEM AND FEATURES

The study of a number of key events and the intervals between them is known as the keystroke dynamics. In order to capture timing features of keystroke, KeyPress and KeyRelease are two most important extracted features.

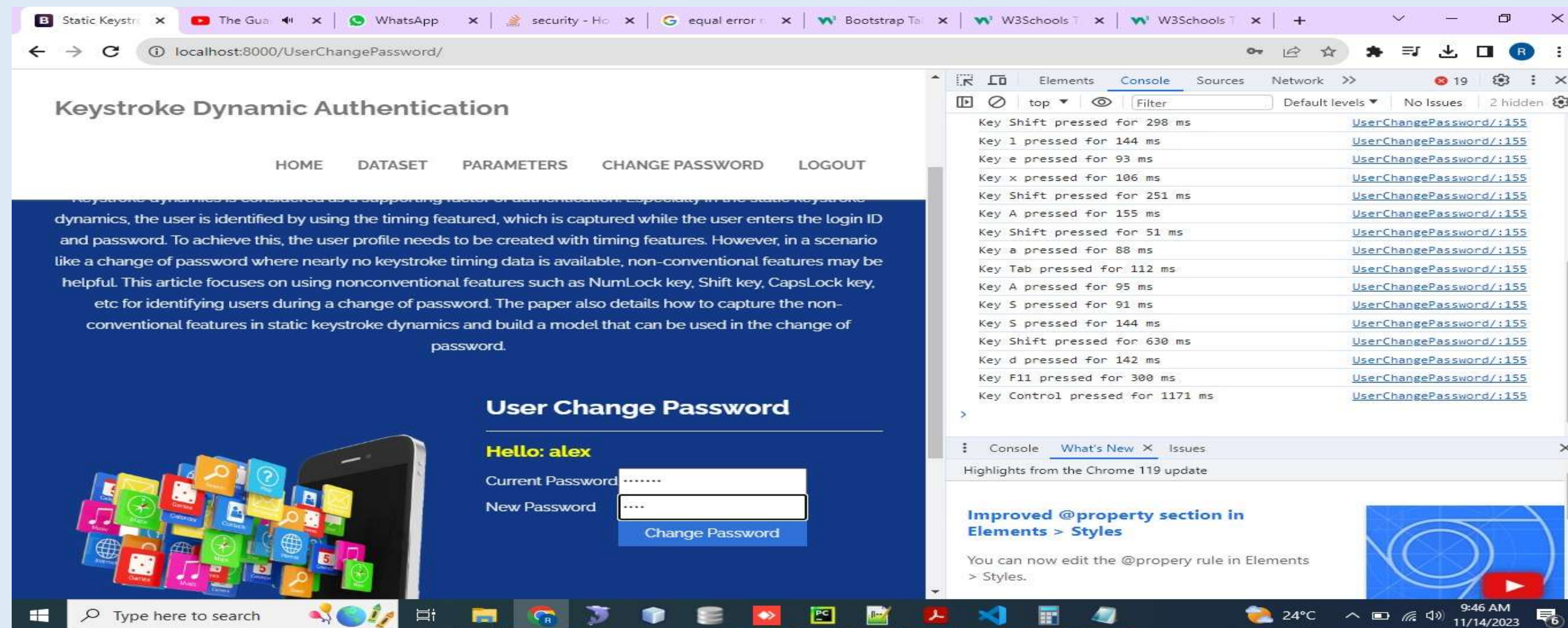
In a keystroke dynamics system, users' keystroke features are first captured to create user profile for him/her. The keystroke dynamic system then analyses users' typing patterns and creates user profile. From the user's typing rhythm different timing features are collected.

The system described in the earlier section is useful while verifying the password. But when the user changes the password, the model derived from the training of different password may not work until a new model is developed for the new password. The trained timing features will be helpful only in verifying the user through their typing behaviour of specific words. Entering login and password being Static keystroke dynamics additional typing information cannot be captured and there is a dependency on the model developed for the specific password.

- › Hold time is a distance between KeyPress and KeyRelease timing
- › UP-Up time is the distance between two consecutive KeyReleases

3. Existing System

- ✓ During enrollment, users establish a baseline profile through static keystroke data.
- ✓ When changing the passwords, users provide dynamic keystroke data by typing a specific prompt.
- ✓ The overall aim is to provide a secure, user-friendly, and privacy-compliant solution for enhanced user authentication during password changes.



4. Disadvantages of Existing System

- ✓ Firstly, keystroke dynamics can be affected by variations in user behavior due to stress, fatigue, or changes in typing patterns, leading to false rejections or acceptances.
- ✓ Secondly, the system may struggle with accommodating users who have inconsistent typing habits or disabilities, reducing accessibility.
- ✓ Additionally, enrollment requires a significant amount of static data, which may lead to user frustration and hinder adoption.

Admin Login:

Keystroke Dynamic Authentication

[HOME](#) [USER](#) [ADMIN](#) [REGISTER](#)

Static Keystroke Dynamic Authentication (SKDA) Model to Authenticate User during Password Change

Keystroke dynamics is considered as a supporting factor of authentication. Especially in the static keystroke dynamics, the user is identified by using the timing featured, which is captured while the user enters the login ID and password. To achieve this, the user profile needs to be created with timing features. However, in a scenario like a change of password where nearly no keystroke timing data is available, non-conventional features may be helpful. This article focuses on using nonconventional features such as NumLock key, Shift key, CapsLock key, etc for identifying users during a change of password. The paper also details how to capture the non-conventional features in static keystroke dynamics and build a model that can be used in the change of password.

Admin Login Form

Login

Reset



5. Proposed System

- ✓ The proposed SKDA system combines static keystroke dynamics and dynamic authentication for enhanced user verification during password changes.
- ✓ The system compares this dynamic data with the baseline to authenticate the user, allowing for a secure password update
- ✓ Emphasis is placed on security measures, positive user experience, continuous improvement, and adherence to privacy regulations with user consent for data collection.

6. Advantages of Proposed Systems

- ✓ Emphasis is placed on security measures, positive user experience, continuous improvement, and adherence to privacy regulations with user consent for data collection.
- ✓ By combining static and dynamic keystroke dynamics, it strengthens security through multi-layered verification, reducing the risk of unauthorized access.
- ✓ The use of a baseline profile ensures that authentication remains accurate over time, even if minor variations in typing occur.
- ✓ The system also supports continuous improvement through adaptive learning, making it more effective with frequent use.

Figure
related
to your
project

7. System Requirements

- ❖ **Operating system** : Windows 10.
- ❖ **Coding Language** : Python.
- ❖ **Front-End** : Html. CSS
- ❖ **Designing** : Html,css,javascript.
- ❖ **Data Base** : SQLite.

8. Implementation

- **MODULES:**

- Admin

The screenshot shows the 'Admin Login Form' on a dark blue background. At the top, the title 'Static Keystroke Dynamic Authentication (SKDA) Model to Authenticate User during Password Change' is displayed. Below the title, a paragraph of text explains the system's purpose. The login form consists of two white input fields: 'Enter Login Id' and 'Enter password'. Below these fields are two blue buttons labeled 'Login' and 'Reset'. The top navigation bar includes links for 'HOME', 'USER', 'ADMIN', and 'REGISTER'.

- > User

The screenshot shows the 'User Login Form' on a dark blue background. At the top, the title 'Static Keystroke Dynamic Authentication (SKDA) Model to Authenticate User during Password Change' is displayed. Below the title, a paragraph of text explains the system's purpose. The login form consists of two white input fields: 'Enter Login Id' and 'Enter password'. Below these fields are two blue buttons labeled 'Login' and 'Reset'. The top navigation bar includes links for 'HOME', 'USER', 'ADMIN', and 'REGISTER'. The URL '127.0.0.1:8000/UserLogin/' is visible in the bottom left corner.

9. Testing / Experimentation

S.no	Test Case	Excepted Result	Result	Remarks(IF Fails)
1	User Register	If User registration successfully.	Pass	If already user email exist then it fails.
2	User Login	If Username and password is correct then it will getting valid page.	Pass	Un Register Users will not logged in.
3	View Parameter Results by User	Parameter Results will be displayed by the user	Pass	Results not true failed
4	View Parameter Results by Admin	Parameter Results will be displayed by the admin	Pass	Results not true Failed
5	Admin login	Admin can login with his login credential. If success he get his home page	Pass	Invalid login details will not allowed here
6	Admin can activate the register users	Admin can activate the register user id	Pass	If user id not found then it won't login.

10. Results

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

11. Future Enhancement

- ✓ The future enhancements for the Static Keystroke Dynamic Authentication (SKDA) model involve a comprehensive strategy to elevate security, usability, and adaptability. By integrating additional behavioral biometrics and leveraging machine learning for continuous refinement, the model aims to keep pace with evolving user behaviors. Adaptive authentication policies, exploration of multi-factor authentication, and real-time anomaly detection contribute to a dynamic and responsive authentication system.

12. Conclusion

- ✓ In static keystroke dynamics, the user is authenticated based on the model generated from the timing features captured while entering the login and password. However, during the change of password, no data related to key press and release for the new password is available. This results in, the model available for static keystroke dynamics for the new password of the user.

13. References

- ✓ R. Joyce and G. Gupta, "Identity authentication based on keystroke latencies," in Communications of the ACM, 33(2), 168-176, 1990.
- ✓ S. Mondal and P. Bours, "Continuous authentication in a real world settings," in Advances in Pattern Recognition, Eighth International Conference, pp. 1-6, 2015.
- ✓ F. Monrose and A. D. Rubin, "Keystroke dynamics as a biometric for authentication," in Future Generation computer systems, 16(4), 351-359, Elsevier Science, 2000.

