Project Title

"Touch-Based Morse Code Password System: Enhancing Accessibility and Usability"

The hypothesis for this project is as follows:

Introducing a touch-based Morse code password system enhances user interaction by providing an intuitive and accessible security mechanism. Furthermore, it can serve as an alternative password input method, especially for users with visible disabilities, while maintaining high usability and adaptability.

Key Elements of the Hypothesis:

1. **Intuitive and User-Friendly**:
    - By using short (.) and long (-) touches, the system offers a natural and intuitive interaction experience.
    - A short learning curve is expected, allowing most users to quickly adapt to the system.
2. **Inclusivity and Accessibility**:
    - The system provides an alternative input method particularly beneficial for visually impaired users.
    - It suits users who may face challenges with physical keyboards or traditional touch-screen inputs.
3. **Security and Flexibility**:
    - The personalized touch patterns maintain the security of the password system.
    - The system allows for diverse pattern combinations, enabling users to create customized, preferred input methods.
4. **Learning Curve Effectiveness**:
    - Experimental data is expected to show a reduction in password input failure rates over time.
    - The system's intuitiveness is hypothesized to improve user experience with minimal practice.

Verification of the Hypothesis:

- To validate the system's intuitiveness, analyze **touch durations (short/long)** and **success rates (success/fail)** to validate the system's intuitiveness.
- Gather user feedback through surveys to evaluate the **usability** and **accessibility** of the system.

Outcomes

- Deliver a functional and intuitive Morse Code Password System built with Python.
    - This part is "Heju's part.iphynb" on GitHub
- Collect and analyze data from 20 participants to evaluate the system's usability and accessibility.
    - This part is "Sean's part.iphynb" on GitHub
- Generate meaningful visualizations to highlight findings and improve the system.

Process of Work

Phase 1: System Development

- **Heju (Lead)**: Designed and developed the Morse Code Password System using Python (Tkinter). Features included password setup, unlocking functionality, and touch duration logic.
- **Sean (Support)**: Provided feedback during the development phase, focusing on usability and seamless data logging integration.

Phase 2: Data Collection and Cleaning

- Each member collected data from 10 participants (20 total), focusing on password attempts, success/failure rates, and touch durations.
- **Sean (Lead)**: Cleaned and organized the data for effective analysis.

  Clarified Data Collection Process: This survey data is “Survey results for 20 participants.xlsx” on GitHub.

  - **Participants**:
    1. 20 individuals aged 18–35, including students, professionals, and individuals with varying levels of technological expertise to simulate diverse user behaviors.
  - **Environment**:
    1. Data collection occurred in controlled environments such as homes or academic settings to minimize external distractions and standardize conditions.
  - **Process**:
    1. Each participant tested 5 unique passwords.
    2. Each password was attempted once to record interaction patterns and error rates.
    3. Participants completed a post-test survey to evaluate the system’s usability and accessibility.

Phase 3: Data Analysis and Visualization

- **Sean (Lead)**: Processed the cleaned data to produce bar charts, pie charts, and histograms to identify usability trends and touch duration patterns.
- **Heju (Support)**: Provided the mechanism to create a file(="touch_durations.csv") when the touch code password system actually ran. Validated and improved the clarity of the visualizations.

Phase 4: Reporting and Presentation Development

- **Collaborative Effort**:
  - Prepared a detailed report.
  - Created a 10-15 minute video presentation, with Heju demonstrating the system and Sean presenting the analysis and visualizations.

List of Software You Use

- **Development**: This part is “Heju’s part.iphynb” on GitHub
  - Python (Tkinter) for GUI and core functionality, emphasizing simplicity and accessibility.
- **Analysis**: This part is “Sean’s part.iphynb” on GitHub
  - Python (Matplotlib, Pandas) for robust data analysis and visual representation.
- **Excel:** To calculate the average mean for survey results.

Roles and Contributions

Heju: Morse Code Password System Development

- Designed and implemented the system’s GUI and touch input logic.
- Ensured accurate real-time logging of user interaction data.
- Collaborated with Sean to align system features with data analysis requirements.

Sean: Data Analysis and Visualization

- Managed data cleaning and analysis from 20 participants.
- Created visualizations to identify patterns in success rates, touch durations, and user behaviors.
- Provided system improvement suggestions based on insights from participant data.

Collaborative Efforts

- Both team members participated in data collection, each gathering data from 10 participants.
- Regular discussions ensured effective integration between system functionality and data analysis.
- Jointly prepared the project report and presentation.

Conclusion

Key Findings from the Analysis:

Password Match Success Rate: The analysis reveals a 73% success rate for password attempts and a 27% failure rate. This indicates that the majority of users were able to input their passwords correctly, highlighting the system's intuitiveness and ease of use.

Touch Duration Distribution: It shows that most users preferred shorter touch durations (less than 0.2 seconds), with the frequency decreasing as the duration increased. This supports our expectation that shorter touches are more intuitive for users.

Short and Long Touch Count: The chart demonstrates that short touches were significantly more frequent than long touches or password-check inputs. This further confirms that users adapted well to the system's short-touch mechanism.

Average Touch Duration by User: The average touch durations varied across users, but most remained within a consistent range, indicating that the system was adaptable to different users' behaviors.

These results demonstrate that the touch-based password system is both user-friendly and effective, with the majority of users quickly adapting to the short-touch mechanism. However, the 27% failure rate highlights opportunities for improvement in reducing errors and enhancing the learning experience for new users. By conducting further tests with a larger and more diverse group, including individuals with disabilities, we can continue to refine and optimize the system.

Additionally, we identified the need for further refinements, such as offering clearer feedback or guidance during the input process. To address this, we collected survey responses from the 20 participants to gain valuable insights into their experiences and identify areas for enhancement.

An average score of 3.7 indicates that most participants found the system easy to use and intuitive. This suggests that the system’s design successfully aligns with user expectations and offers a straightforward interaction experience.

An average score of 4.25 underscores the system’s strong potential as an inclusive tool for users with disabilities. This highlights the system's effectiveness in addressing accessibility challenges and its adaptability to diverse user needs.

This project highlights the potential of combining innovative system development with real-world data analysis. By focusing on usability and inclusivity, Heju and Sean demonstrated the practical applications of a touch-based password system and its value for diverse user groups of smart devices.