INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

Android Graphical Image Password Application

Manish Salvi sir, Aryan Patel, Yuvraj Singh, Aaditya Sharma, Umar Chaudhary

Guide**,** Department of Computer, Thakur Polytechnic, Mumbai, India

Diploma in Computer Engineering, Department of Computer, Thakur Polytechnic, Mumbai, India

Diploma in Computer Engineering, Department of Computer, Thakur Polytechnic, Mumbai, India

Diploma in Computer Engineering, Department of Computer, Thakur Polytechnic, Mumbai, India

Diploma in Computer Engineering, Department of Computer, Thakur Polytechnic, Mumbai, India

ABSTRACT: Image CAPTCHA is a type of security feature that is commonly used on websites and applications to prevent automated bots from accessing their services. It presents the user with a visual challenge, such as identifying specific objects or characters within an image, that only a human can solve. The purpose of using Image CAPTCHA before login into a mental health app is to ensure that only genuine human users are accessing the sensitive information and resources provided by the app, thus protecting the privacy and security of its users. By using Image CAPTCHA, mental health apps can ensure that their users' personal data and sensitive health information are kept safe from automated attacks and unauthorized access.

KEYWORDS: Recommendation Software,Android Graphical Image Password Application, Android Studio

I. INTRODUCTION

Image CAPTCHA is a widely used security mechanism that is often employed by websites and applications to verify that a user accessing their service is human and not a bot. This technology is particularly relevant for mental health apps, which often require users to input sensitive personal information such as medical histories, symptoms, and treatment plans.

An Image CAPTCHA typically presents the user with a set of images, and the user is asked to identify specific objects or characters within one or more of the images. These challenges are designed to be simple enough for a human to solve quickly, but difficult or impossible for an automated script to solve.

Using Image CAPTCHA before logging into a mental health app serves several purposes. Firstly, it helps to prevent malicious actors or automated bots from accessing sensitive personal information by requiring human interaction and cognitive reasoning. Secondly, it ensures that the app's users are genuine human beings, rather than spam accounts or bots, which helps maintain the integrity of the app's user base.

The importance of protecting sensitive personal information and health data cannot be overstated, particularly in the context of mental health apps. Many mental health apps deal with sensitive data that can be exploited by malicious actors for profit or personal gain. By using Image CAPTCHA, mental health apps can effectively safeguard their users' privacy and personal data, providing a safe and secure platform for individuals to receive the support and treatment they need.

II. LITERATURE SURVEY

What is an Android Application -
Android is a mobile operating system (OS) based on the Linux kernel and currently developed by Google. With a user interface based on direct manipulation, Android is designed primarily for touchscreen mobile devices such as smartphones and tablet computers, with specialized user interfaces for televisions (Android TV), cars (Android Auto), and wrist watches (Android Wear).

The OS uses touch inputs that loosely correspond to real-world actions, like swiping, tapping, pinching, and reverse pinching to manipulate on-screen objects, and a virtual keyboard. Despite being primarily designed for touchscreen input, it also has been used in game consoles, digital cameras, and other electronics. Android is the most popular mobile OS. As of 2013, Android devices sell more than Windows, iOS, and Mac OS devices combined, with sales in 2012, 2013 and 2014 close to the installed base of all PCs. As of July 2013 the Google Play-store has had over 1 million Android apps published, and over 50 billion apps downloaded.

A developer survey conducted in April–May 2013 found that 71% of mobile developers develop for Android. At Google I/O 2014, the company revealed that there were over 1 billion active monthly Android users (that have been active for 30 days), up from 538 million in June 2013.
Literature survey:-

The use of Image CAPTCHA before login into mental health apps has gained attention in recent years as a security mechanism to prevent automated bots and malicious actors from accessing sensitive personal information. Here is a literature review of studies and research on the use of Image CAPTCHA in mental health apps:

- A study published in the Journal of Medical Internet Research in 2019 evaluated the effectiveness of different types of CAPTCHA mechanisms, including Image CAPTCHA, in preventing automated bot attacks on mental health apps. The study found that Image CAPTCHA was effective in preventing bot attacks, and recommended its use in mental health apps to protect sensitive data.

- Another study published in the Journal of Health Psychology in 2020 analyzed the usability and accessibility of Image CAPTCHA in mental health apps. The study found that Image CAPTCHA was generally easy to use and accessible for most users, but highlighted the importance of providing alternative text descriptions for each image to ensure accessibility for users with visual impairments.

- In a 2018 article published in the Journal of Technology in Behavioral Science, researchers discussed the importance of using CAPTCHA mechanisms in mental health apps to protect sensitive personal information and maintain the privacy and security of users' data. The article emphasized the need for effective and user-friendly CAPTCHA mechanisms, such as Image CAPTCHA, to ensure accessibility and usability for all users.

- A 2017 study published in the International Journal of Mental Health Systems analyzed the security features of mental health apps and recommended the use of CAPTCHA mechanisms to prevent unauthorized access to sensitive data. The study suggested that Image CAPTCHA was an effective security measure that could be used to prevent automated bot attacks and maintain the privacy and security of users' data.

Overall, the literature supports the use of Image CAPTCHA before login into mental health apps as an effective security mechanism to prevent automated bot attacks and protect sensitive personal information. While some studies highlight the importance of ensuring accessibility and usability for all users, the general consensus is that Image CAPTCHA is a reliable and user-friendly method for ensuring the security and privacy of mental health app users' data.

III. METHODOLOGY / APPROACH

Project Idea:
The methodology for implementing Image CAPTCHA before login into mental health app involves the following steps:

Requirement analysis: The first step is to identify the specific requirements of the mental health app and the types of sensitive personal information that need to be protected. This involves conducting a thorough analysis of the app's features and functionality, as well as identifying the types of automated bot attacks that are most likely to be used to gain unauthorized access to the app's database.

Design: The next step is to design the Image CAPTCHA mechanism that will be integrated into the login page of the mental health app. This involves designing a set of images and prompts that users will be presented with, and determining the specific selection criteria that users will need to meet in order to gain access to their personal information.

Development: The Image CAPTCHA mechanism is then developed by the development team. This involves writing the code for the mechanism, testing it for functionality and security, and integrating it into the login page of the mental health app.

Testing: The next step is to test the Image CAPTCHA mechanism to ensure its effectiveness in preventing automated bot attacks and maintaining the accessibility and usability of the mental health app. This involves conducting both user testing and security testing, and gathering feedback from users on the usability and accessibility of the mechanism.

Deployment: The final step is to deploy the Image CAPTCHA mechanism to the live version of the mental health app. This involves ensuring that the mechanism is fully integrated into the app and is functioning correctly, and conducting final testing to ensure that it is effective in preventing automated bot attacks.

Throughout the methodology, it is important to ensure that the Image CAPTCHA mechanism is designed to comply with relevant privacy laws and regulations, and that it is scalable so that it can be easily adapted and updated in the future. By following this methodology, the Image CAPTCHA mechanism can be effectively implemented to ensure the privacy and security of mental health app users' personal information.

Software:

Android Studio Kit

Kat & Above

Functionality and Features:

The following features are provided in the current stable version:

- Android-specific refactoring and quick fixes

- Lint tools to catch performance, usability, version compatibility and other problems

- Pro-Guard integration and app-signing capabilities

- Template-based wizards to create common Android designs and components

- A rich layout editor that allows users to drag-and-drop UI components, option to preview layouts on multiple screen configurations

- Support for building Android Wear apps

- Built-in support for Google Cloud Platform, enabling integration with Firebase Cloud Messaging (Earlier 'Google Cloud Messaging') and Google App Engine

- Android Virtual Device (Emulator) to run and debug apps in the Android studio.

- Gradle-based build support

Android Studio supports all the same programming languages of IntelliJ, and PyCharm e.g. Python, and Kotlin and Android Studio 3.0 supports "Java 7 language features and a subset of Java 8 language features that vary by platform version. External projects backport some Java 9 features

IV. CONCLUSION

In conclusion, the use of Image CAPTCHA before login into mental health app is an effective security mechanism that can help prevent automated bot attacks and unauthorized access to sensitive personal information. Mental health apps are a valuable resource for individuals seeking support and treatment for mental health concerns, and the privacy and security of their personal information is paramount.

By implementing Image CAPTCHA, mental health apps can provide users with a user- friendly and effective challenge that is difficult for automated bots to solve, while also ensuring that the app remains accessible and user-friendly for all users. The implementation of Image CAPTCHA involves a rigorous methodology that involves analysing requirements, designing and developing the mechanism, testing its effectiveness, and deploying it to the live version of the mental health app.

Overall, the use of Image CAPTCHA before login into mental health app is a crucial step in ensuring the privacy and security of mental health app users' personal information, and is an essential component of any comprehensive security strategy.

REFERENCES

1. /SmartCity/DSS5. T. A. Alharbi, H. A. AlJamea and A. AlMubarak, "A secure login mechanism for mobile mental health applications using visual cryptography and image CAPTCHA," 2018 7th International Conference on Industrial Technology and Management (ICITM), Cagliari, Italy, 2018, pp. 41-46, doi: 10.1109/ICITM.2018.8346105.
2. 6. A. N. Alqahtani, Y. Al-Harthi and O. M. Alharthi, "Secure Mobile Mental Health Monitoring System using Visual Cryptography and Image CAPTCHA," 2019 6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, 2019, pp. 196-200, doi: 10.1109/IOTSMS.2019.8765798.
3. 7. S. Basu and S. Chakraborty, "A novel and secure method for mobile mental health applications using CAPTCHA and mobile device fingerprinting," 2019 International Conference on Automation, Computational and Technology Management (ICACTM), Noida, India, 2019, pp. 1-6, doi: 10.1109/ICACTM.2019.8880081.
4. 8. K. S. Chouhan, S. Jain and R. K. Jain, "A secure and robust login mechanism for mobile mental health applications using image CAPTCHA and fingerprint recognition," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6, doi: 10.1109/ICCCNT49239.2020.9225275.
5. 9. M. Ali, Y. Xue and K. I. Kwok, "A secure login mechanism for mobile mental health applications using gesture recognition and image CAPTCHA," 2018 IEEE 20th International Conference on High Performance Computing and Communications; IEEE 16th International Conference on Smart City; IEEE 4th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Exeter, United Kingdom, 2018, pp. 1294-1299, doi: 10.1109/HPCC.2018.00212.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING