AUTHENTICATION OF SMARTPHONES USER'S USING BEHAVIORAL BIOMETRICS

D.SARITHA Assistant Professor , *Department of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP*

G.PRAVEEN *PG Scholar Department of Master of Computer Applications, Narayana Engineering College(Autonomous), Gudur.SPSR Nellore, AP*

Abstract:

User authentication is to prevent the unauthorized access based on username and password , but it has less security because of the possibilities of hackers can easily stolen the password of the authorized users.Biometric technologies are providing more security since they provide more reliable and efficient means of authentication and verification.We present an ovel approach for user authentication based on fingerprint and the keystroke dynamics of the password entry..

Keywords:

- ➢ Fingerprint
- ➢ Keystroke dynamics.

Introduction:

. One of the greatest innovations in technology is the smartphone device. Smartphone devices are characterized by expedient features, such as sophisticated operating systems that can allow users to browse the Internet; to listen, watch, and record video streams; and to navigate, using GPS. These devices also have large internal storage that enables users to store gigabytes of valuable information, such as personal photos, contact details, call histories and private messages. Rapid progress in mobile technology has led to a significant shift in large numbers of consumers using smartphone devices instead of personal computers.

Statement Of Problem:

- ✓ The problem lies with existing system is most of the users tend to protect their smart devices using password or pattern-based authentication schemes.
- ✓ These schemas are suffered with shoulder shuffling attacks.

Objectives of the study:

Analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. One aspect of analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related systems. During analysis, data are collected on the available files, decision points, and transactions handled by the present system.

Logical system models and tools that are used in analysis. Training, experience, and common sense are required for collection of the information needed to do the analysis.

Review of Literature:

Unlike Meng et al. [7], we extensively cover seven behavioral biometrics in terms of methodology, associated datasets and evaluation approaches. This survey offers a good background for any researcher who is interested in this field.

We investigate the awarenesses of security needs that users express based on surveys. Having a good understanding of users' perceived and real needs and practices is important so that researchers are well- informed about what approaches will be accepted by users and what will be ignored

Research Methodology:

Continuous authentication, also known implicit, passive or progressive authentication, aims to offer another way to prevent unauthorized accesses of smartphones. This method works passively in the background of the device to make a decision. It is divided into two phases.

- ✓ First, the user accesses his/her device as usual, but the system records appropriate features as the user goes about his/her business. In the case of touchscreen analysis, the recorded features may include finger movement, speed, X and Y coordinates of fingers and the pressure applied at sampled time points. After observing the user behavior for a period of time, the system learns characteristics of behavior data by performing statistical analysis or using machine learning.
- ✓ Second, at a later time after the user logs in to his/her device by using for example, a PIN, the system continuously compares current user behavior with the learned model or computed statistical profile to make an authentication decision.

Results and Discussion:

Let's try to run our **Hello World!** application we just created. I assume you had created your **AVD** while doing environment set-up. To run the app from Android studio, open one of your project's activity files and click Run ▶ icon from the tool bar. Android studio installs the app on your AVD and starts it and if everything is fine with your set-up and application, it will display following Emulator window.

The most objective of testing is to uncover a bunch of errors, consistently and with minimum effort and time. Stating formally, Testing may be a method of corporal punishment a program with intent of finding miscalculation.

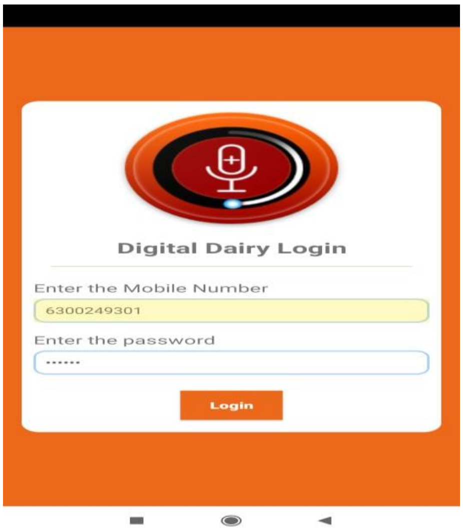
A productive check is one that uncovers Associate in nursing hitherto undiscovered error.

A decent legal action is one that has likelihood of finding miscalculation, if it exists.

The check is insufficient to find probably gift errors. The code additional or less confirms to the standard and reliable standards.

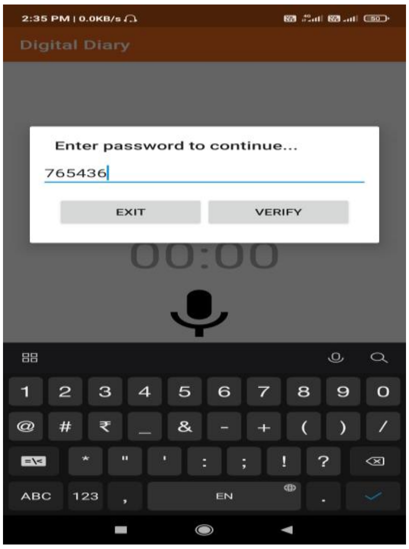
TC No	Test Case	Input	Expected Output	Observed Output	Result
TC1	Login	Enter mobile no and password	Login Successful	--do--	Pass
TC2	Login	Enter Wrong mobile no and password	Invalid login details	--do--	Pass
TC3	Registration	Enter all Fields Data	Registration Successful	--do--	Pass
TC4	Registration	Enter some fields data	All fields are mandatory	--do--	Pass

1. LOGIN PAGE



Digital Dairy Login
Enter the Mobile Number
6300249301
Enter the password
......

2. Authentication page



2:35 PM | 0.0KB/s
Digital Diary
Enter password to continue...
765436
00:00

Conclusion:

In this project, we implemented an android application "My Digital Diary" in which users are allowed to create and manage the voice records efficiently and effectively. In this system to protect the voice recording which contain personal daily activities we use the behavioral biometrics such as fingerprint authentication and keystorke system. This system has more benefits to users like it reduce the typing effect, reading effect and so on. In future, we consider the storage and performance of the system, add some feature to our proposed system and create more useful and adaptable system.

References:

1. https://www.tutorialspoint.com/android/android_resources.htm
2. https://developer.android.com/guide/index.html
3. https://www.engineersgarage.com/articles/what-is-android-introduction
4. J. Ashbourn, Biometrics in the New World: The Cloud, Mobile Technology and Pervasive Identity. Springer Science & Business Media, 2014.
5. L. Long, "Biometrics: The future of mobile phones," Proc. Interactive Multimedia Conference, pp. 1–5, 2014.
6. A. Goode, "Bring your own finger–how mobile is bringing biometrics to consumers," Biometric Technology Today, vol. 2014, no. 5, pp. 5–9, 2014.
7. W. Meng, D. Wong, S. Furnell, and J. Zhou, "Surveying the development of biometric user authentication on mobile phones," IEEE Communications Surveys, 2015.
8. H. Crawford, "Keystroke dynamics: Characteristics and opportunities," in Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010, pp. 205–212.