Authentication of Smartphone Users Using Behavioral Biometrics

Abstract:

Smartphones and tablets have become ubiquitous in our daily lives. Smartphones, in particular, have become more than personal assistants. These devices have provided new avenues for consumers to play, work and socialize whenever and wherever they want. Smartphones are small in size; so they are easy to handle and to stow and carry in users’ pockets or purses. However, mobile devices are also susceptible to various problems. One of the greatest concerns is the possibility of breach in security and privacy if the device is seized by an outside party. It is possible that threats can come from friends as well as strangers. Due to the size of smart devices, they can be easily lost and may expose details of users’ private lives. In addition, this might enable pervasive observation or imitation of one’s movements and activities, such as sending messages to contacts, accessing private communication, shopping with a credit card, and relaying information about where one has been. This paper highlights the potential risks that occur when smartphones are stolen or seized, discusses the concept of continuous authentication, and analyzes current approaches and mechanisms of behavioral biometrics with respect to methodology, associated datasets and evaluation approaches.
Existing system:

The tremendous increase in the number of consumers who are buying smartphones has pushed these devices to the top of the market, and they now lead all other electronic devices in terms of sales. According to the International Data Corporation (IDC), the total number of shipments in the second quarter of 2015 reached 337.2 million smartphones worldwide, an increase of 11.6% compared to the same quarter in 2014. The second quarter in 2015 has the second highest quarterly total on record. The number of smartphones is shipped predicted to rise to 1,928.4 million in 2019.

Disadvantage:

As much as these devices have gained in popularity and enhanced users’ productivity and consumption of entertainment, the security of these devices continues to be a major concern for manufacturers and users alike.
The above picture represent Approaches to Authenticate Users

Proposed system:

In Proposed System we focus on comprehensively summarizing the state-of-the-art in improving a smartphone’s security based on continuous authentication using...
behavioral biometrics. Behavioral biometrics, as defined in III-B, use behavioral traits of a subject like how one touches screen, walks, talks, signs a signature, and types to identify a subject. Each subject is expected to differ from all others when analyzed using one or more of these features. In the following sections, we discuss in depth four types: keystroke, touchscreen behavior, gait and handwaving, and also introduce other types such as voice, signature and profiling. A powerful argument for behavioral biometrics is that it can assist in continuous and passive authentication without requiring additional hardware. As a result, behavioral authentication is likely to be cheaper than using physiological biometrics. In the following sections, we will discuss several examples of behavioral biometrics. These are based on touchscreen behavior, gait, keystroke, handwaving, voice, profiling and signature.

Advantages:

✓ Advantage of this method focus on multiple characteristics and secure against a variety of attacks, while making the security system easy to use and adapted to each owner.
Conclusion :

The growing number of users of smart device is resulting in an increasing amount of private information being stored inside each such devices. Numerous problems in security and privacy are constantly being raised. To resolve these issues, researchers have implemented many methods including continuous authentication approaches based on user behavior. This paper has discussed and compared a number of existing solutions from several perspectives. New methods must focus on multiple characteristics and secure against a variety of attacks, while making the security system easy to use and adapted to each owner.

Hardware Specification :

- System : Pentium IV 2.4 GHz.
- Hard Disk : 40 GB.
- Floppy Drive : 44 Mb.
- Monitor : 15 VGA Colour.
- Mouse : Logitech
- Ram : 512 Mb.
- MOBILE : ANDROID
Software Specification:

- Coding Language: Java 1.7
- Tool Kit: Android 2.3 ABOVE
- IDE: Android Studio

Reference:


