Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 113 (2017) 202–209

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2017)

# Identifying Smartphone Users based on their Activity Patterns via Mobile Sensing

M. Ehatisham-ul-Haq[a], Muhammad Awais Azam[a,*], Usman Naeem[b], Shafiq ur Rèhman[b,c], Asra Khalid[d]

[a]*Faculty of Telecom and Information Engineering, University of Engineering and Technology, Taxila, Punjab, Pakistan*
[b]*School of Architecture, Computing and Engineering, University of East London, E16 2RD, United Kingdom*
[c]*Department of Applied Physics and Electronics, Umeå University, SE-90187, Sweden*
[d]*Department of Computer Science, COMSATS Institute of Information Technology, Wah Campus, Pakistan*

**Abstract**

Smartphones are ubiquitous devices that enable users to perform many of their routine tasks anytime and anywhere. With the advancement in information technology, smartphones are now equipped with sensing and networking capabilities that provide context-awareness for a wide range of applications. Due to ease of use and access, many users are using smartphones to store their private data, such as personal identifiers and bank account details. This type of sensitive data can be vulnerable if the device gets lost or stolen. The existing methods for securing mobile devices, including passwords, PINs and pattern locks are susceptible to many bouts such as smudge attacks. This paper proposes a novel framework to protect sensitive data on smartphones by identifying smartphone users based on their behavioral traits using smartphone embedded sensors. A series of experiments have been conducted for validating the proposed framework, which demonstrate its effectiveness.


Peer-review under responsibility of the Conference Program Chairs.

*Keywords:* Activity Recognition; Behavioral Biometrics; Continuous Sensing; Mobile Device Security; Data Privacy; Mobile Sensing; Ubiquitous Computing; User Identification;

## 1. Introduction

Smartphones are context-aware devices that are becoming more and more dominant with ever-growing computing, sensing and networking capabilities. They provide ubiquity and assist users in accomplishing their daily

* Muhammad Awais Azam. Ph: +92-312-5151200
*E-mail address:* awais.azam@uettaxila.edu.pk

1877-0509 
Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.08.349

routine tasks, including sending and receiving e-mails, playing games and socializing anytime and anywhere. The pervasiveness of smartphones has changed the entire structure of people's everyday lives even users with disabilities[1,2]. Market research on usage of smartphones depicts that the number of smartphones sold has surpassed the number of laptops sold worldwide[3]. Instead of using personal computers, people are now using smartphones for storing most of their personal data so that it can be accessed effortlessly at anytime and anywhere when required. With the progress in usage of smartphones, users have become anxious about the secrecy of their data and information available through these devices. Unfortunately, most widely used methods for protecting smartphones such as passwords, PINs, patterns locks and fingerprint scans provide limited security. They are exposed to many attacks, such as guessing[4] (passwords and PINs), spoofing[5] (fingerprint scans) and side channel attacks such as video capture[6], reflection[7] and smudge attacks[8]. They prompt users to deal with the device actively for entering some pieces of information for validation, which frustrates user. Also, these approaches are futile to use after login because of their failure in detecting and recognizing a user once he/she has passed the point of entry[9]. Therefore, it has become critical to find out viable solutions for these challenges to protect sensitive data available through these devices. Continuous and passive mobile sensing offers a way to use behavioral biometrics to identify a smartphone user continuously[11]. Behavioral biometrics schemes aim to identify the characteristics of a user behavior that possess a definite pattern over a period such as hand movements and waving patterns[13], voice[14], signature[15], touchscreen interactions[16] and gait patterns[17]. The major issues in developing a continuous mobile sensing system for identifying smartphone users are as follows:

- Orientation sensitivity of smartphone inertial sensors as shown in Fig. 1
- Efficiently learning activity patterns from noisy data
- Incorporating sensor data into a biometric authentication setup on a smartphone
- Adaption of the user identification model to a new user in real-time

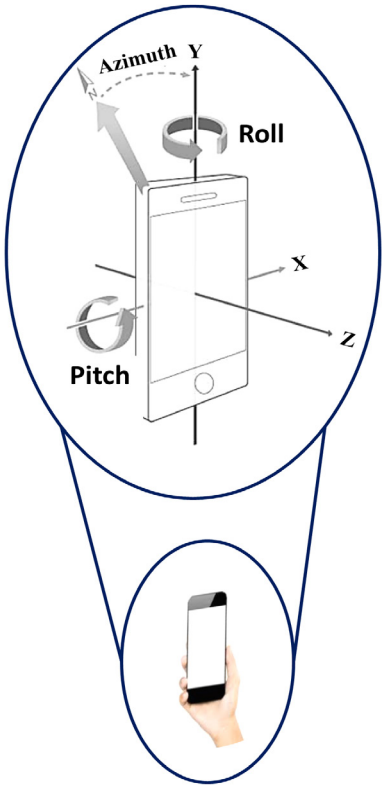


Fig. 1. Smartphone inertial sensors are orientation sensitive. The axes of the smartphone inertial sensors change their directions if the orientation of the smartphone is changed. Hence, the readings of these sensors are different for varying orientations of the smartphone.