Touch Panel with Integrated Fingerprint Sensors Based User Identity Management

Tao Feng, Varun Prakash, and Weidong Shi
Computer Science Department, University of Houston
Email: {tfeng3, larryshi}@cs.uh.edu, vsprakash@uh.edu

***Abstract*—In this paper, to enhance identity acquisition procedures in smartphones and make the process transparent to the user, a novel User Identity Sensing approach leveraging the unified fingerprint enabled touch panel that combines multiple capacitive TFT based fingerprint sensors directly with the touch screen panel of the smartphone is proposed. The solution passively fulfills mobile users identity management during natural user-device touch interactions and requires neither password nor extra actions from the user, which makes it highly user friendly. To demonstrate the feasibility of such a unified, user identity sensing based design, an investigation of the hardware metrics is performed. Simulation experiments are conducted to evaluate the system with touch data collected from 25 smartphone users. The resulting observations and simulation results provide guidance for an efficient design of the hardware and criteria that need to be satisfied for the development of an operational prototype.**

***Index Terms*—Smartphone, User Identity Sensing, Touch Interaction, Touchscreen, Fingerprint**

I. Introduction

There has been a recent surge in the usage of smartphones, which not only have the computing capabilities of desktops of a few years back and the ability to maintain connectivity over a variety of network interfaces, but also aims to continuously improve their user experience capabilities. Smartphones are quickly replacing personal computers, both in numbers and average engagement period. According to the market analysis and predictions, in 2015, there will be 1.5 billion smartphones in use worldwide [1]. The wide adoption of smartphones creates strong demands of phone based user identity sensing that can be applied to improve user experiences and collaboration (e.g., smart multi-user phone, intelligent casual multi-user interfaces), design user friendly access control (e.g., burden free phone access and control) and carry out smoother and safer online activities (e.g, password free access for web sites from a phone). Many approaches have been proposed for smartphone based user identity sensing by leveraging either the smartphone sensors such as camera, motion sensor [15], multi-touch panel [18], microphone, location sensor [16] or using behavior patterns.

Ideal smartphone user identity sensing techniques should posses the following characteristics, (i) robust and accurate smartphone user identity verification; (ii) non-intrusive and low user burden; and (iii) compatibility with the slim form factor of today's smartphones. Although current solutions suffice the provision of isolated profiles for multiple users, it also creates an overhead by burdening the users to remember the required login credentials. More importantly, text and password based identity authentication can prove to be of little or no effect when passwords are compromised or unintentionally leaked to unwarranted users. This aspect demands the need for an authentication credential that is unique in the true sense. Based on the intricate details of the solution, the smartphone might also face a deteriorated performance caused by the discrete user identification procedures if there is a need for frequent transitions between multiple, unique and fully functional profiles for different users.

In order to address the above challenges, we propose a novel user identity sensing approach for touch based mobile devices that is user transparent, burden free and demonstrates high levels of accuracy by leveraging the emerging techniques of transparent electronic sensors. Taking advantage of the fact that smartphone interactions by the user, which is mainly through the touch screen interface, and fingerprint sensing are both touch based, a novel user identity sensing approach can be designed to detect user identity from fingerprint data opportunistically sensed during natural user device touch interactions. Such approach provides many advantages over other alternative or competing user identity sensing techniques. Firstly, it provides stronger and more reliable identity detection performance because fingerprint is well established as a reliable and highly accurate data source for identity verification. Secondly, it is transparent to the mobile user and non-intrusive. Thirdly, it incurs neither physical (e.g., extra steps/actions that a user has to take) nor cognitive burden (e.g., remembering a password) on the mobile user, making it more user friendly and responsive than the other approaches.

The main contributions of our work include:

- Design of a novel mobile identity sensing approach that integrates transparent fingerprint sensors with touch panel for opportunistic identity detection from natural user-mobile device touch interactions;
- Identification and proposition of solutions to tackle some of the must-be-addressed challenges for implementing the proposed opportunistic identity sensing technology such as optimal placement of fingerprint sensors.
- Empirical study and feasibility evaluation of the proposed solution for opportunistic identity sensing. This is achieved by a careful step by step study of common and conventional ways of smartphone usage by a group of participants and using the data collected by their interactions with the touch panel.
- Insights gathered from the experiments and detailed simulation studies that provide valuable guidance and requirements for the hardware design and implementation.

II. Background

A. Touchscreen

Touchscreens have been widely adopted recently as the solution for interacting with portable devices such as smartphones,

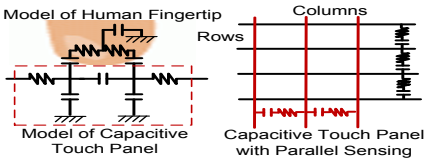


Fig. 1. Left: The equivalent model of the capacitive touch panel and human fingertip. Right: Simple model for the capacitive touch panel with parallel sensing.

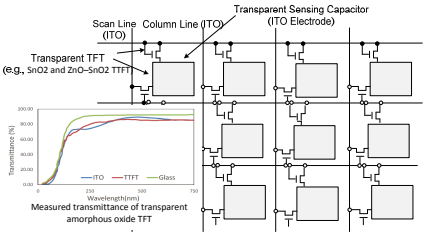


Fig. 2. Equivalent Circuit Model of Transparent TFT Fingerprint Sensing Array (For each sensing cell, all the components can be made from transparent materials, ITOs and transparent thin-film transistors)[5]

tablets, notebooks, navigation systems, and so on. Touchscreens utilized in consumer portable devices are mainly add-on types where the touchscreens are separated from the display panel. Design and manufacture of add-on type touchscreens is a mature industry with many commercially available sensing methods. Common sensing methods include: resistive [3], capacitive [17], acoustic-wave [2], and infrared based touch sensing techniques. Among these, the capacitive based method is increasingly popular because of its sensitivity, durability, and ability to detect multi-touches. The typical response time of a capacitive touch panel is 4ms.

B. Fingerprint Sensors and Transparent Electronics

The optical type of fingerprint sensor requires a lens system and is hard to implement in a small package at a low cost. One alternative is a TFT (thin film transistor) based fingerprint sensor. TFT technique is well known for creating large size displays. The technique puts ICs directly onto a glass substrate. It is the most cost effective and scalable way for creating fingerprint sensors that can cover larger area than the standard CMOS process based approach. In the past, several capacitive fingerprint sensor prototypes and products were developed using poly-Si TFTs [12]. Performance characteristics of some fabricated capacitive fingerprint sensing devices are shown in Table I.

In the last few years, a revolutionary trend in electronic materials is occurring, which is to implement TFTs using transparent materials and transparent electronic fabrication process. Transparent electronics is a rapidly developing technology that employs wide band-gap semiconductors for the realization of invisible circuits [8]. It enables the electronic manufacturers to design and build a variety of transparent electronic devices such as transparent TFT display (already successfully adopted by the consumer market), transparent fingerprint readers, transparent CMOS, or even transparent physical DRAM [14]. Transparent fingerprint sensors are built based on the same design and fabrication principle as the other transparent TFT based electronic devices. Figure 2 shows an abstract circuit model of transparent TFT based fingerprint sensing array. All the components are made from transparent materials. Someone may ask, why transparent fingerprint sensing didn't exist before? When compared with the abstract circuit model of multi-touch panel (also made from transparent material, ITO) in Figure 1, one can notice that there are two transparent thin film transistors involved in each sensing cell. The discovery of how to fabricate transparent thin film transistor is one of the key enabling techniques for transparent fingerprint sensors.

Reference	Cell Size	Resolution	Response	Frequency
[22]	42 μm	64 x 256	3ms	4MHz
[19]	81.6 μm	124 x 166	2ms	Not Mentioned
[12]	60 μm	320 x 250	160ms	500kHz
[11]	66 μm	304 x 304	200ms	250kHz
[20]	50 μm	224 x 256	20ms	Not Mentioned

TABLE I
PERFORMANCE DATA OF SOME ACTUAL FINGERPRINT SENSORS

III. DESIGN

We designed a solution to integrate multiple capacitive TFT fingerprint sensors with a touchscreen and tackled the speed and data capture challenges with two new techniques. A block diagram of the proposed high speed TFT fingerprint sensors integrated with a touchscreen is shown in Figure 3. Multiple capacitive TFT fingerprint sensors can be overlayed on top of a touchscreen. Each TFT fingerprint sensor contains a matrix of capacitive fingerprint sensing cells. The TFT fingerprint sensors are abstracted from the user by using transparent TFTs. Placements of the TFT fingerprint sensors are optimized in such a way that the chances of capturing touches during the user-mobile device interactions are maximized. All the TFT fingerprint sensors are controlled by a controller chip. At the very beginning, only the touchscreen is in fully powered-on state. Fingerprint sensors are idle by default. When the finger tip is inside the region covered by a fingerprint sensor, its location will be recorded by the touchscreen controller first. Then the fingerprint sensor controller will be notified. Typically, the touchscreen response time is less than 4ms [4]. Furthermore, for minimizing interferences, the touchscreen can use a different touch technique such as resistive multi-touch sensing, acoustic-wave or infrared based touch sensing.

Algorithm 1 Pseudocode: Opportunistic Capture of Fingerprints

```
while true do
    Detect Touch Point (x,y);
    Transform Touchscreen (x,y) to Fingerprint Sensor Row and Column Addresses (r,c)
    if Fingertip Location (r,c) Inside the Areas of a Fingerprint Sensor then
        Drive Fingerprint Sensors and Capture Fingertip Data;
        Evaluate Quality of the Captured Data and Apply Fingerprint Match;
        if Fingerprint Matches with the Owner then
            Continue;
        else
            Take Pre-defined Response Action;
        end if
    end if
end while
```

Each fingerprint sensor and cell has its unique column address and line address. The fingerprint controller can translate a touchscreen location (position in touchscreen X-axis and Y-axis) into a pair that consists of a line address and a column address. The line address decoder in Figure 3 can decode

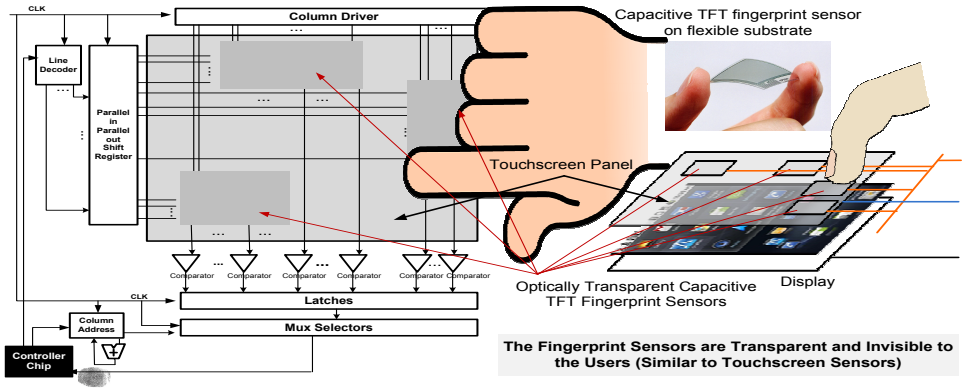
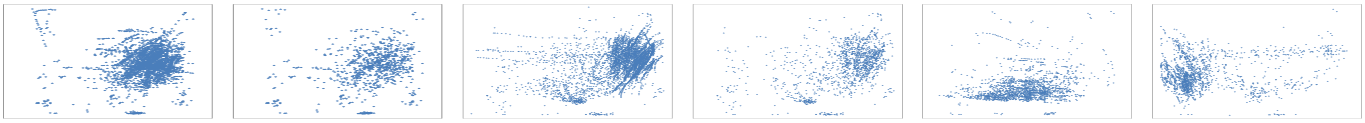


Fig. 3. Touchpanel with Integrated Transparent Capacitive Fingerprint Sensors



(a) User1's touches (b) User1's touches above 7 ms (c) User2's touches (d) User2's touches above 7 ms (e) User3's touches above 7 ms: landscape mode user (f) User4's touches above 7 ms: left handed user

Fig. 5. Touch Distributions: Data from Four Representative Users

(a) Pitch: Touch Angles (b) Yaw: Touch Directions (c) Roll: Touch Orientations

Fig. 4. Different types of physical touch actions commonly performed by users. The picture on top represents the initial position of the finger in contact with the touchscreen and the picture at the bottom shows the final position after the transition.

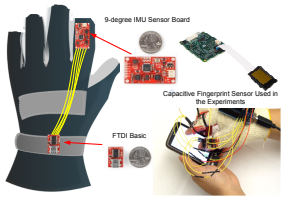


Fig. 6. Sensor Glove and Finderprint Sensor Used for Experiments

a line address and send the decoded output to a parallel-in parallel-out shift register. The shift register will enable one row of capacitive sensing cells at a time. All of the sensing cells in the enabled row will be addressed during a clock cycle and disabled after the results of the sensing cells are converted into digital values and fed into the latches that are situated at the end of each column. For each sensor cell, a comparator compares its voltage output with a reference voltage and stores a binary result into the corresponding latch. The design supports parallel accesses of the sensor cells at an enabled row therefore maximizing fingerprint scan speed. Pixel results stored in the latches are selected and transmitted to the fingerprint controller. For minimizing the amount of data transferred, the fingerprint controller computes a pair of column addresses as the beginning and the end column addresses. Only results stored in the latches within the selected columns are transferred to the fingerprint controller. Using parallel addressing and selected data transfer, one can greatly improve fingerprint capture speed. The described driving and controlling system is compatible with any TFT based capacitive fingerprint sensor built using transparent components.

The processing steps are summarized in algorithm 1. User identity sensing is applied both for unlocking a mobile device and afterward (opportunistic).

IV. Fingerprint Sensor Placement

In this section, we discuss how to optimally place the sensors in order to capture as many valid fingerprints as possible with limited sensor areas. We conducted two studies, (i) *touch density and touch distribution user study*, which aims to find out the most frequently touched parts of the touchscreen, touch duration (time period a finger resting on the touchscreen surface) and the touch angles during normal user-mobile device interactions; and (ii) *sensitivity of user identity sensing performance to data completeness and the other factors*, which aims to find out the recognition rates of incomplete fingerprints and fingerprints of different touch angles. Figure 7 shows the detailed experiments and procedures.

A. Touch Density and Touch Distribution User Study

Due to the cost of the fingerprint sensors, we need to use the least amount of fingerprint sensor coverage areas to attain the highest possible user identity sensing performance. For such a purpose, we rely on density profiles of touches to identify which parts of the touchscreen are been used most frequently, and to identify if these touches can support capture of fingerprints and fingerprint verification by considering factors such as touch time, touch angles and orientations. We collect the touch duration and 3D angle information, including **touch angles**, **directions** and **finger orientations** of each touch as shown in Figure 4.

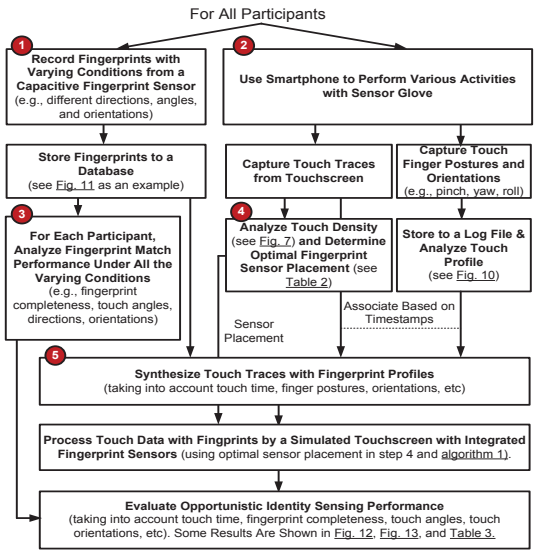


Fig. 7. Procedures for Evaluating Opportunistic User Identity Sensing

1) Experiment: In this study, we used multi-touch enabled smartphone devices with the Android operating system (Figure 7, step 2 and step 4). The user can control and interact with the Android smartphone through the touchscreen. The touchscreen has an overall response latency below 4 ms. All touch events made by the user were logged using evdev support in Android Linux. Moreover we used 9DOF Razor IMU to assist data collection as shown in Figure 6. The 9DOF razor IMU can collect data of finger postures. It can capture finger orientations, angles, and directions using four sensors - a single-axis gyro, a dual-axis gyro, a triple-axis accelerometer, and a triple-axis magnetometer. The outputs of all the sensors were processed by an on-board chip and sent to the host desktop via Bluetooth. 25 subjects participated in the study. The participants were asked to perform regular mobile device operations such as making phone calls, checking emails, web browsing, etc. Each of the participants was required to use the Android Phone for at least two hours.

We collected some attributes of a user's interactions with the smartphone's touch screen such as touch angles, directions, finger orientations, touch duration and touch coordinates. The results were saved with time stamps synchronized with the logged touch events sent from the Android device using Android Debug Bridge (ADB). Two profiles were used to store the users' input information: (i) a touch density profile that contains touchscreen's X and Y coordinates and time information, and (ii) a touch characteristic profile that contained the touch angle, direction and finger orientation information.

2) Results: Six of the collected touch density profiles from 4 users are shown in Figure 5. Figure 5(a) and Figure 5(c) show touch distributions from two representative users. Figure 5(b) and Figure 5(d) show only those touches where the fingers stayed at the same place for more than 7ms (3ms for deactivating the touchscreen sensor and activating the fingerprint sensor, and 4ms for capturing the fingerprint data). From Figure 5(b) and Figure 5(d), one can easily observer that there are a lot of similarities in touch distributions between the two users. Figure 5(e) and Figure 5(f) respectively show the touch density of a landscape mode user and a left-handed user. Comparing the touch distributions of all the users, although differences do exist, many touch areas are still shared across the users.

Statistics of touch characteristic profiles for the 25 participants are shown in Figure 8. Figure 8(a) shows that significant percentages of their touches stayed still on the touchscreen for long period and can support fingerprint capture and recognition. In addition, from Figure 8(b), Figure 8(c) and Figure 8(d), for most of the time, all the users touched the touchscreen with an angle, a touch direction or a finger orientation below 60 degrees. Which help us limit the angle variation in the next study.

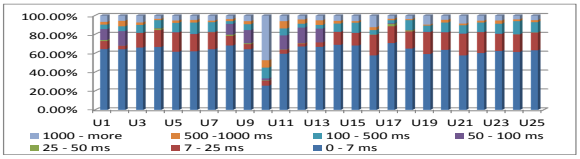
B. Sensitivity Study of User Identity Sensing Performance

Fingerprints captured during natural mobile device usage most likely have variations in touch angles, finger orientations, and directions. It is possible that these factors would affect the user identity sensing performance. Furthermore, based on our design, the fingerprint sensor would not cover the whole touchscreen for cost considerations. So in certain situations, the fingerprint sensor has to sense user identity from incomplete fingerprint data. Therefore, we conducted studies to evaluate the fingerprint recognition rates in both cases of incomplete fingerprints and fingerprints of different touch angles.

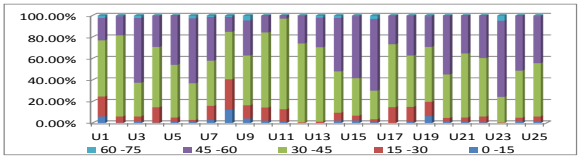
1) Experiment: We used the 9DOF Razor IMU and the Upek Eikon Touch 700 to collect the touch angles and the fingerprint raw data respectively. The same 25 subjects were asked to use different touch angles, directions and finger orientations when collecting their fingerprints (Figure 7, step 1 and step 3).

For evaluation, we collected: (i) Raw fingerprints: We collected fingerprints of 25 users from the Upek Eikon Touch 700 combined with the 9DOF Razor IMU. The data were captured under different touch angles (0 to 75 degrees), touch directions (-75 to 75 degrees), and finger orientations (-75 to 75 degrees) guide by the result of previous study. From each participant, we collected on average 62 fingerprints with different touch angles, finger orientations, and touch directions; and (ii) Partial fingerprints: We defined five incomplete fingerprint settings from 1mm to 5mm. The incomplete fingerprint setting is a representation of the longest length of an incomplete fingerprint out of the capture area of a fingerprint sensor. We synthesized incomplete fingerprints by applying the above five settings in all directions, and removing the out-of-range data. We acquired a total of 84,924 different incomplete fingerprint samples for further analysis.

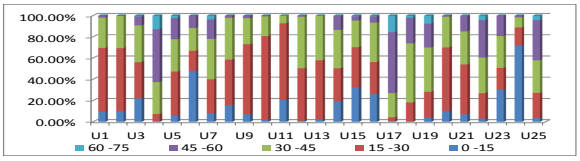
2) Results: Through the analysis, we found that if the fingerprint data is complete and the touch angle, touch direction and finger orientation are below 60 degrees, the recognition rate is touch angle, finger orientation, and touch direction independent, as shown in Figure 9. Even when the touch angle is above the threshold, accuracy would remain the same or change only slightly for most the users. However, during natural usage, sometimes, fingerprints captured from the sensors would contain only partial data, which means that a part of the fingerprint was out of the area that the fingerprint sensor could sense. So when evaluating fingerprint recognition rates, it is necessary to take recognition rates of incomplete fingerprints into consideration. By analyzing the incomplete fingerprint samples, we obtained the statistical results shown in Figure 10. The results suggest that as the missing border of



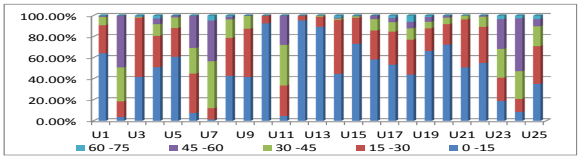
(a) Duration Distributions of Touches



(b) Distribution of Touch Angles



(c) Distribution of Finger Orientations



(d) Distribution of Finger Directions

Fig. 8. Statistics of Touch Profiles from Twenty-Five Participants

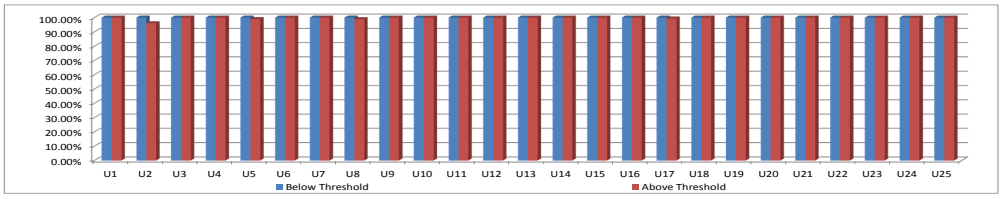


Fig. 9. Fingerprint Recognition Rates Based on Touch Angles, Directions and Orientations, Threshold means - Angle:60, Direction:60, and Orientation:60

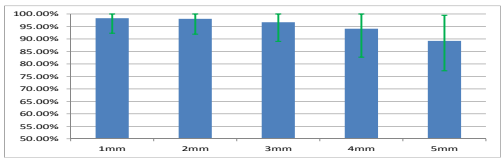


Fig. 10. Partial Fingerprint Recognition Rates

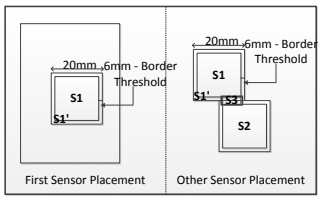


Fig. 11. Illustration of Fingerprint Sensor Placement Approach

incomplete fingerprint grows larger, the fingerprint recognition rates will drop because incomplete fingerprints may not be admitted for recognition. In the evaluation, we used a setting of 4mm for admitting captured fingerprints based on the consideration of both accuracy and efficiency.

C. Approach of Sensor Placement

For sensor placement, one consideration is to place the fingerprint sensors where critical or primary buttons of the mobile device will be displayed, such as the unlock button, the home button, or the cancel button. This design can make an unregistered user unable to unlock the mobile device or can only login to privacy-free interface and file system, and a registered user switch to his/her own interface and file system, because fingerprint recognition cannot be bypassed. In addition, we need to place the sensors in the areas with the highest touch density for better opportunistic sensing results. Furthermore, each sensor area should be sufficiently large to minimize the number of incomplete fingerprints. So we chose the size of a fingerprint sensor unit to be 20mm x 20mm. As shown in the left part of Figure 11 that describes the placement of a first fingerprint sensor, all touch points falling into the area denoted by $S1$ can produce valid samples for fingerprint recognition. Touch points in the area outside $S1$, but inside the sensor's capture area, $S1'$ are ignored for fingerprint recognition because these touches will lead to incomplete fingerprints that have low recognition rates.

We used a brute force approach for sensor placement. For placing the first sensor, we first set the up-left corner of the sensor at $(1, 1)$ which is the up-left coordinate of the touchscreen, compute the number of valid touch points that fall into $S1$ according to the set of touch points, P, collected from the participants, and record the number in a matrix. After we traverse all the pixel locations of the touchscreen, we can get a result matrix that provides a summary of which touchscreen region is mostly touched by the participants. The maximum of the matrix is the place we should place the first fingerprint sensor. Then we remove all the touch points in $S1$ from set P, reset the matrix to zeros, and repeat the process for placing the second fingerprint sensor. The right column of Figure 11 shows the strategy for placing additional fingerprint sensors. Two neighboring sensors, Sensor 1 and Sensor 2 will have an extra valid touch area S3. The area of $S3$ can be calculated using the following equations, assuming that x_1 and y_1 denote the up-left of Sensor 1, x_2 and y_2 denote the up-left of Sensor 2, and L denotes the *4mm - border threshold*:

- If Sensor 1 and Sensor 2 share a vertical boundary: Up-Left of $S3$: $(max(x_2 + L, x_1 + L), min(y_1 + 20 - L, y_2 + 20 - L))$; Right-Down of S3: $(min(x_2 + 20 - L, x_1 + 20 - L), max(y_2 + L, y_1 + L))$; and
- If Sensor 1 and Sensor 2 share a horizontal boundary: Up-Left of $S3$: $(min(x_1 + 20 - L, x_2 + 20 - L), max(y_2 + L, y_1 + L))$; Right-Down of S3: $(max(x_2 + L, x_1 + L), min(y_1 + 20 - L, y_2 + 20 - L))$.

So when coming to placing an additional Sensor n on the touchscreen, we repeat the same process. During the traversal, if the current sensor does not share boundaries with any

Area Percentage	HTC 110mm*60mm	HTC 85mm*55mm
15%	25.18%	18.29%
20%	35.92%	33.52%
25%	45.62%	39.12%

TABLE II
SENSOR AREAS AND TOUCH COVERAGE

previous sensors, we just calculate the number of valid touches in area Sn and record the value in the touch matrix. If it shares a boundary with a previously placed fingerprint sensor, we calculate the valid touches in Sn and the neighboring area described above. When the traversal is complete, we choose the maximum of the matrix and remove all the touch points in the valid touch area and neighboring areas if the newly added fingerprint sensor shares boundary with the other sensors and set the matrix to zero. The results of simulated sensor placement using touchscreen sizes of two HTC smartphone models are shown in Table II. The results indicate that there is a trade-off between fingerprint sensor coverage and the number of captured touches. Based on Table II, 20% would be a good choice from both the cost and area coverage perspectives.

V. ANALYSIS

Based on the results acquired from the previous two user studies, in this section, we explore and analyze the design requirements of the novel opportunistic user identity sensing approach. Touch data collected from the participants are used to determine how many touches the system, under different metrics settings, needs to verify a mobile user's identity from natural touch interactions. Based on the design, when a smartphone is in the locked mode, it can only be unlocked by touching an unlock button situated over a fingerprint sensor. In this case, the FAR (false acceptance rate) is 0.01% and FRR (false reject rate) is 0% based on the fingerprint recognition algorithms.

For user identity sensing from natural touch interactions, we run simulation on the combined collected touch, angle and fingerprint data over 100,000 cases, the result is shown in Table III. The results are based on the display and touchscreen settings of the $110mm*60mm$ HTC phone. We used a border threshold of 4mm. To explore variables such as fingerprint sensing time and sensor coverage, we experimented with actual fingerprint sensing time obtained from Table I. As indicated by the results, on average, user identity can be detected after very few touches for all the tested settings. Opportunistic user identity sensing is feasible as long as the fingerprint capture latency is below 200ms. The user identity sensing performance is stable when the sensor coverage is between 15% to 25%. In terms of FAR (false acceptance rate) and FRR (false reject rate), a sensor coverage below 20% is not sufficient to be user friendly because the FRR is higher. Based on the results, a design of 20% sensor coverage is fairly enough to support highly accurate user identity sensing from natural touches.

VI. RELATED WORK

Traditionally, user identity sensing during normal human machine interactions is done through analyzing keyboard or mouse inputs [6]. With the increasing popularity of portable devices, several approaches have been proposed for user identity sensing by leveraging the sensors that can be found in a mobile device. For example, in [15], the authors described an approach to identify users of portable devices from gait patterns using accelerometers. In [16], smartphone location histories were used to detect the user. As touch becomes the main smartphone interaction interface, user identity sensing approaches based on touch inputs were proposed [18]. In [7], the authors propose to improve strength of swipe with features extracted from the touches. In [9], [10], Feng et al. also introduced continuous and implicit user identity authentication by touch input data and biometric integrated touch-display.

For fingerprint and touchscreen input integration, in [21], Wang et al. studied the touch input properties of users. Recently, some researches used fingerprint sensors to reduce the touch inaccuracy of touchscreens [13]. Our paper is the first one in the literature that explores the feasibility and design to integrate fingerprint based user identity sensing with natural touch interactions using touch interaction data collected from real users.

Sensor Coverage (percentage)	Response	Average Touches for User Identity Sensing	FAR in 10 Touches	FRR in 10 Touches
15%	2ms	3.76	0.01%	2.98%
15%	3ms	3.78	0.01%	3.00%
15%	20ms	3.80	0.01%	3.02%
15%	160ms	4.53	0.01%	3.52%
15%	200ms	4.62	0.01%	3.63%
20%	2ms	2.76	0.01%	0.13%
20%	3ms	2.76	0.01%	0.13%
20%	20ms	2.98	0.01%	0.13%
20%	160ms	3.20	0.01%	0.14%
20%	200ms	3.32	0.01%	0.14%
25%	2ms	2.16	0.01%	0.11%
25%	3ms	2.18	0.01%	0.12%
25%	20ms	2.24	0.01%	0.12%
25%	160ms	2.48	0.01%	0.12%
25%	200ms	2.50	0.01%	0.13%

TABLE III
PERFORMANCE OF USER IDENTITY SENSING FROM NATURAL TOUCHES UNDER DIFFERENT SENSING INTERVALS

VII. CONCLUSIONS AND FUTURE WORK

This paper explores a novel integrated design and approach, based on combining a touchpanel with transparent TFT based fingerprint sensors for opportunistic and ambient user identity sensing that requires neither password nor extra operation steps from the mobile users. The results of simulation experiments based on the data collected in live scenarions of smartphone usage from 25 human subjects provides us with the knowledge of the importance of particular factors that need to be considered to architect and induct the hardware. Based on the results of our design exploration, we discovered that: (i) Opportunistic user identity sensing is feasible as long as the fingerprint capture latency is below 200ms; (ii) A design of 20% sensor coverage is fairly enough to support highly accurate user identity sensing from natural touches. Our exploration results provide encouraging statistics and guidance for the development of an integrable user identity sensing hardware module to meet the user identity sensing performance requirements. In terms of the future work, we are in the process of fabricating the sensors described in the paper.

REFERENCES

[1] Worldwide smartphone markets: 2011 to 2015 - analysis, data, insight and forecasts. http://www.researchandmarkets.com/research/7a1189/worldwide_smartpho.

[2] R. Adler and P. Desmares. An economical touch panel using saw absorption. *Ultrasonics, Ferroelectrics and Frequency Control, IEEE Transactions on*, 34(2):195 –201, march 1987.

[3] R. Aguilar and G. Meijer. Fast interface electronics for a resistive touch-screen. In *Sensors, 2002. Proceedings of IEEE*, volume 2, pages 1360 – 1363 vol.2, 2002.

[4] Atmel. Touchscreen Controllers - Parameters. http://www.atmel.com/products/touchsolutions/touchscreens/default.aspx, 2012.

[5] W.-S. Cheong, S.-M. Yoon, C.-S. Hwang, and H. Y. Chu. High-mobility transparent sno2 and zno-sno2 thin-film transistors with sio2/al2o3 gate insulators. *Jpn J Appl Phys*, 48(4):04C090–04C090–4, apr 2009.

[6] N. L. Clarke and S. M. Furnell. Authenticating mobile phone users using keystroke analysis. *Int. J. Inf. Secur.*, 6:1–14, December 2006.

[7] A. De Luca, A. Hang, F. Brudy, C. Lindner, and H. Hussmann. Touch me once and i know it's you!: implicit authentication based on touch screen patterns. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*.

[8] A. Facchetti and T. J. Marks. *Transparent electronics : from synthesis to applications*. Wiley, Chichester, U.K., 2010.

[9] T. Feng, Z. Liu, B. Carbunar, D. Boumber, and W. Shi. Continuous remote mobile identity management using biometric integrated touch-display. *45th Annual IEEE/ACM International Symposium on Microarchitecture Workshops (MICROW)*, 0:55–62, 2012.

[10] T. Feng, Z. Liu, K.-A. Kwon, W. Shi, B. Carbunar, Y. Jiang, and N. Nguyen. Continuous mobile authentication using touchscreen gestures. In *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, pages 451–456, 2012.

[11] H. Hara, M. Sakurai, M. Miyasaka, S. W. B. Tam, S. Inoue, and T. Shimoda. Low temperature polycrystalline silicon 'tft' fingerprint sensor with integrated comparator circuit. In *Solid-State Circuits Conference - ESSCIRC 2004*, pages 403–406, 2004.

[12] R. Hashido, A. Suzuki, A. Iwata, T. Okamoto, Y. Satoh, and M. Inoue. A capacitive fingerprint sensor chip using low-temperature poly-si tfts on a glass substrate and a novel and unique sensing method. *IEEE Journal of Solid-State Circuits*, 38, 2003.

[13] C. Holz and P. Baudisch. The generalized perceived input point model and how to double touch accuracy by extracting fingerprints. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 581–590. ACM, 2010.

[14] S.-J. Kim, J.-M. Song, and J.-S. Lee. Transparent organic thin-film transistors and nonvolatile memory devices fabricated on flexible plastic substrates. *J. Mater. Chem.*, 21:14516–14522, 2011.

[15] J. Mantyjarvi, M. Lindholm, E. Vildjiounaite, S. marja Makela, and H. Ailisto. Identifying users of portable devices from gait pattern with accelerometers. In *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2005.

[16] P. Marcus, M. Kessel, and C. Linnhoff-Popien. Securing mobile device-based machine interactions with user location histories. In *Security and Privacy in Mobile Information and Communication Systems*. Springer Berlin Heidelberg, 2012.

[17] J.-Y. Ruan, P.-P. Chao, and W.-P. Chen. A multi-touch interface circuit for a large-sized capacitive touch panel. In *Sensors, 2010 IEEE*, pages 309 –314, nov. 2010.

[18] W. Shi, J. Yang, Y. Jiang, F. Yang, and Y. Xiong. Senguard: Passive user identification on smartphones using multiple sensors. In *IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications*, pages 141–148, 2011.

[19] S. Shigematsu, H. Morimura, Y. Tanabe, T. Adachi, and K. Machida. A single-chip fingerprint sensor and identifier. *J. Solid-State Circuits*, 34(12):1852–1857, 1999.

[20] T. Shimamura, H. Morimura, S. Shigematsu, M. Nakanishi, and K. Machida. Capacitive-sensing circuit technique for image quality improvement on fingerprint sensor lsis. *J. Solid-State Circuits*, 45(5):1080–1087, 2010.

[21] F. Wang and X. Ren. Empirical evaluation for finger input properties in multi-touch interaction. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 1063–1072, 2009.

[22] J. woo Lee, S. Member, D. jin Min, J. Kim, and W. Kim. A 600-dpi capacitive fingerprint sensor chip and image-synthesis technique. *IEEE Journal of Solid-State Circuits*, 34:469–475, 1999.