Development of a typing behaviour recognition mechanism on Android

Xuan Huang, Geoffrey Lund, and Andrew Sapeluk
School of Computing and Engineering Systems, University of Abertay Dundee,
Dundee, Scotland, UK
x.huang@abertay.ac.uk
g.lund@abertay.ac.uk
a.sapeluk@abertay.ac.uk

Abstract—**This paper proposes a biometric authentication system which use password based and behavioural traits (typing behaviours) authentication technology to establish user's identity on a mobile phone. The proposed system can work on the latest smart phone platform. It uses mobile devices to capture user's keystroke data and transmit it to web server. The authentication engine will establish if a user is genuine or fraudulent. In addition, a standard deviation "α" has been defined which aims to achieve the balance between security and usability. Experimental results indicate that the developed authentication system is highly reliable and very secure with an equal error rate is below 7.5%.**

Keywords-Biometric Authentication; Typing Behaviour; Smart Phones; Keystroke Analysis

I. INTRODUCTION

With the development of mobile communication technology, mobile phone is not just a device to call or text a friend, it is capable of supporting a wide variety of services. Many of these services require the users to establish their identities on the phone, and at the same time, mobile theft is also rising: some new crime means such as password theft and remote control are threatening personal information security. Therefore, we need to have a new biological recognition technology to ensure the security of information transmission.

A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioural characteristic possessed by user [1]. Biometric approaches are typically subdivided into two categories, physiological and behavioural [2]. Physiological biometrics includes fingerprints, facial features, or iris patterns. Conversely, behavioural biometrics attempts to characterise the way of an individual acts, such as speaking, typing, or signing their name. At present, many biometric authentication techniques have been widely used and accepted, but each method has its own scope of application, not all suitable for the mobile authentication. Consider to the specific hardware configuration of mobile devices — most of mobile phone has a keyboard, so typing behaviour recognition techniques can be used in a mobile authentication system [3].

Currently, the most widely deployed authentication methods are passwords and PINs (Personal Identification Numbers) [2]. However, the poor use of passwords and PINs has been widely documented [4]. The typing behaviour recognition is based on username and password, but also combines with the keystroke analysis technique. The new recognition technology can achieve individual authentication in human-machine interaction process (such as individual operate the keyboard of computers or mobile phones). In 1986, the first keystroke recognition system was proposed by Garcia [5], who has successfully designed a personal identification apparatus by using keystroke recognition technique. And in Blender and others [6]work, they found that if the system can achieve recording and analysing user's input mode at the same time with user password identification, this dual protection mode will not only guarantees the user's actual space and data security, but also effectively prevent the invasion of hackers. On the other side, typing behaviour

recognition is not only used on desktop or laptop, Clarke and Furnell's [2] work is based on mobile devices, and they have noted that neural networks superior pattern classification method, but that mobile devices lack the computing power necessary to employ a neural network in situations where the processing is done on the device itself [7].

Overview the current researches, most of the studies are based on desktop and laptop keystroke dynamics [4], [5], [8], and others are based on numeric keyboard phone or Personal Digital Assistants (PDA) [2], [9], [10]. The typing behaviour recognition system proposed in this paper is implemented on the latest smart phone platform, and it also uses multi-level authentication mechanism which can achieves the balance between security and usability.

The main task of this paper is to develop a mobile application and use the metrics based on typing behaviour to establish the identity of the user on a mobile phone. Therefore, a number of objectives should be includes:

- Develop a mobile application which can run on smart phone platform (like Android phone, iphone or blackberry phone).
- Multi-level authentication mechanism.
- Balance between security and usability.

II. TYPING BEHAVIOUR RECOGNITION ON MOBILE DEVICE

A. *Authenticating user using keystroke analysis*

The operating principle of a typing behaviour recognition system is: when user input username or password through their computer or mobile phone keyboard, the system not only identifies the password to log on, but also analysis the keystroke data (usually how long they hold the key and the intervals between each key were pressed). Primarily in this study, two keystroke characteristics can be utilised to solve the interactions between individuals and mobile phone keyboards.

• *The keystroke latency*, or time between successive keystrokes. It is a measure of the amount of time between when a key is released and the subsequent key is pressed.
• *The key hold-time*, or the time to press and release a key. It is a measure of the amount of time between when a key is pressed and when the same key is released.

These two keystroke characteristics can be consider as the standard metrics in the system [7]. Both metrics are common in studies that examine keystroke dynamics on desktop and laptop keyboards. Particularly in this paper, these two metrics can be captured from a full-size mobile phone keyboard.

In keystroke analysis process, the keystroke data is recorded when user type in the password. So for example if the password is "abertay2011", there are 10 "*keystroke latency"* and 11 "*Key hold-time*" are recorded. In the training phase the user must enter their username and password 6 times to register. When the system captures user's registration data, it will record the duration and interval and calculate the average time. Subsequently, the data will be sent to web server though wireless internet connection and then generate an xml document in database. In order to study the feasibility of typing behaviour recognition, the researcher firstly registers an administrator account: use "abertaytest" as username and "abertay2011" as password, follow on a number of volunteers were asked to login use the same username and password. We choose two participant's "*Key hold-time*" and compare it with the researcher's, the difference between them can be shown in figure 1.

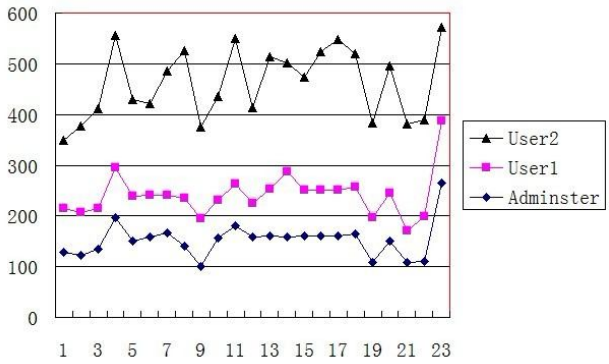

Figure1. The comparison result between each participant

In figure 1, it shows each participant has their own input timing pattern, and they are different. Compared with the researcher's typing pattern, we can found two facts are different in the database, because there is a fairly consistent upward and downward pattern to the lines of each participant. Obviously, some participants tended to press certain keys for much longer than others, and also require much longer transition time to press the next key. In this system, each user has to type in the

same username and password 6 times to register; and the captured keystroke data will be stored in database as user's pattern. This pattern contains two keystroke metrics: Pattern Duration (also consider as *the key hold-time)* and Pattern Interval (also consider as *the keystroke latency)*. When user's typing pattern compared with the target, there are two kinds of authentication results: Accept or Reject.

- *To accept a user:*

Pattern Duration/α ＜ Attempt Duration ＜ Pattern Duration×α Pattern Interval/α ＜ Attempt Interval ＜ Pattern Interval×α

- *To reject a user:*

Attempt Duration＞Pattern Duration×α latencies ＞Pattern Interval×α

Attempt Duration＜Pattern Duration /α latencies ＜Pattern Interval /α

In the algorithm above, we introduce a new parameter "α" which is a variable value can determines the FRR (False rejection rate) and FAR (False acceptance rate) of the system. Whenever a mobile application requires to access any secure data the user may be required to enter some token to prove it is them. When we change the "α" value, the FAR and FRR changed as well. The lower false acceptance rate means the system is more secure; and the higher false rejection rate means the system is easier to reject the valid user. Therefore, other crux of this research work is how to define the "α" value to achieve the balance between security and usability.

B. Multi-level authentication mechanism

In order to improve system performance and authentication efficiency, two security mechanisms should be imperative: set up alert level and achieve the balance between usability and security.

1) Authentication level in the system

The model has 4 alert levels. A transaction is assessed for risk and this defines the alert-level required to approve the transaction. In this paper, risk is synonymous with value of the transaction. Table 1 below shows the "α" value and transactions value at each alert level.

TABLE I. POTENTIAL PARAMETERS FOR INCLUSION INTO THE MULTI-LEVEL AUTHENTICATION MODEL

Alert Level	Transaction Value	"α" Value
0	Low	/
1	Medium	4
2	High	3
3	Very high	2

It is argued that for any user they can balance their expected security for a transaction against the ease of use. Within the model below we are suggesting 4 levels model:

Level 0 - no security required other than just having the phone

Level 1 - simple security of "α"=4, which will reduce the FRR, it is easier for the user to log in the system.

Level 2 - medium security of "α"=3.

Level 3 - higher security of "α"=2. Low FAR means the system is security, but also easier to reject the user's attempts.

2) UI-balance between security and usability

Whenever a mobile application requires to access any secure data the user may be required to enter some token to prove it is them. In the typing behaviour recognition system, the user must input the username and password and the lower value of "α" the more secure the application. However the lower "α" value the less useable the application. Using the safe analogy; if the user puts all his money in a safe, whenever they require 20p for a paper, the "α" value can be set as 4. This is the same as the user being requested for a low risk low value transaction. On the other extreme for a high value transaction many users will accept the "α" value set as 2 which can reduce the FAR.

C. System design and achievement

The typing behaviour recognition system model include two parts: one is client side, the keystroke data capture work is achieved by a Flex application which can runs on Android phone, Iphone or blackberry phone; system database and authentication engine works in the web server. The software development environment is based upon: Microsoft Visual Studio 2008, C#, Flash builder 4.5, ActionScript and XML. These are standard

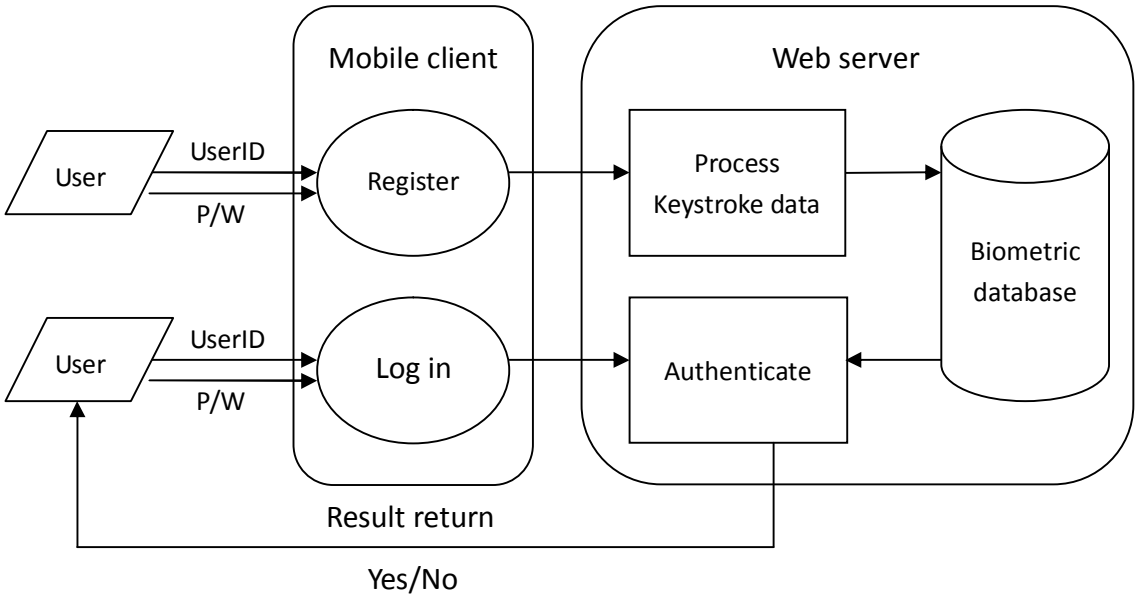

Figure 2. The flow chart of typing behaviour recognition system

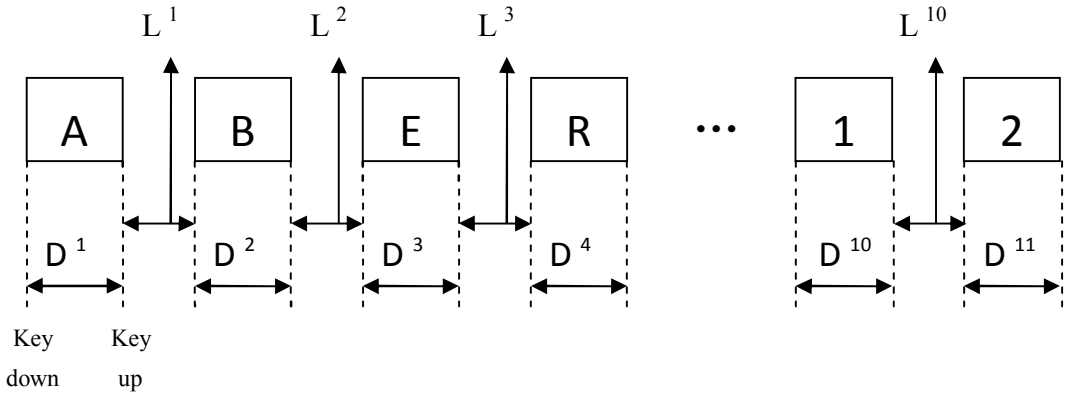

Figure 3. The duration time and latency time in keystroke data(L^1=Latency time^1, D^1=duration time^1)

specifications necessary for providing an environment for mounting and implementing applications downloaded via the wireless Internet on the mobile communication terminal. The figure 2 describes the working process of the system. There are two interfaces on the client side: registration and login. The registration page will ask user to type in a username and password six times. Then the client side will analysis the keystroke data. Figure 3 shows the duration time and latency time in user's keystroke data. If a user uses "abertaytest" as username and "abertay2012" as password, there are 132 duration times and 120 latency times need to record. In order to improve the data process efficiency, the client side will firstly calculates the mean times; and then upload it to web server. In the mechanism we proposed:

Pattern Average Duration= （Duration t1+ Duration t2+ ……+ Duration t6）/ 6
Pattern Average Interval= （Interval t1+ Interval t2+ ……+ Interval t6）/ 6

According to the principle described in figure 3, it can calculate the duration time and latency time as the follows algorithm:

The duration time^1 = keyUpTime ^{1} – keyDownTime^1
Latency time^1 = keyDown^2 – keyUp^1

After data analysis, the username and password plus the keystroke data are written in an xml document and stored into the database. This provides the reference point or signature for that user. When user wants to log in, the client will capture the keystroke data and upload to web server. Follow on, the authentication engine will analysis

the keystroke attempts and compare it with user's pattern, return an authentication result at last. Each user has 3 potential attempts at the password, each is checked at the server for accuracy of the letters and the latency between letters is within bounds. Again if OK then the transaction is accepted, if not then a denial message is passed to the phone and displayed to the user.

III. EXPERIMENTAL WORK

A. *Aim of the work*

In order to evaluate the effectiveness of the typing behaviour recognition in a mobile environment, it is necessary to get biometric data from the volunteers. In this phase, there have 40 volunteers test the system and their keystroke data were recorded. The participants are students or any other researchers in the University and they will be told the purpose of the work and asked to fill out a current form. The total of 40 participants aged from 22 to 55 years old and their mobile phone use experience is from 3 years to 10 years and the average is 6.2 years. The main purpose of these experiments is to find out the FAR and FRR when "α" value changed, and also the best way to achieve the balance between usability and security.

B. *Methodology*

The experimental work can be dividing into three groups, the "α" value has been defined as 2 in group 1 and the value changed to 3 and 4 in the next two groups. At the same time, there are three steps of work in each group:

(1) when user first time uses the system, it is required to enter user name and password six times to register;

(2) the second step is validation, participants will try to login use their own user name and password, it is used to test the false rejection rate;

(3) in the last step, each participant will be asked to log in again use the specified user name and password which is set by the researcher.

This experiment can help researcher to account the false acceptance rate of the system. When calculating the results, all 40 participants register and login their account successfully. From the experimental results gained from group one, we can find when the "α" value set to 2, there are 12 participants tried more than twice to login, that means false rejection happened 12 times and the FRR is 30%. Conversely, false acceptance didn't happened, this means that the system has not let any unauthorised users access. The screenshot of experimental interface is shown in figure 4.

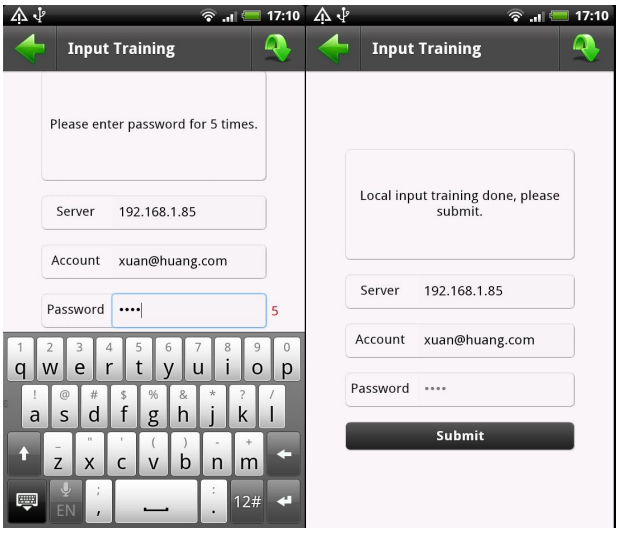

Figure 4. The user interface on Android phone

C. *Results*

When analysis the experimental result, it was found in experiment 1, if user's attempt duration and interval time is two times greater than the pattern average time or less than half of the mean, the access request will be denied. During the experiment, first time user will enter their username and password. When users were unable to achieve a "verified" outcome, the false rejection happened and they will be asked to login again. Subsequently, each participant were asked to login using other participant's username and password, if access successful, the false acceptance will happen. In experiment 2, the 'α' value in section 2 will be changed to 3 which means user's attempt duration and interval time is three times greater than the pattern average time, the access request will be denied; Similarly in experiment 3, 'α' value will be changed to 4. Different 'α' value will affect the FRR and FAR in the system, the experimental results are shown in table 2 which illustrates the difference between them.

Figure 5 displays the FAR and FRR changed in each of the experiment, from this diagram we can see all change directions have been plotted and these two lines crossed when "α" value come to 3.8, at that point FAR equal to FRR which means the Equal Error Rate (ERR) is

TABLE II. THE FRR AND FAR IN DIFFERENT EXPERIMENT

	Alert level	'α' value	False rejection (FRR)	False acceptance (FAR)
Experiment 1	3	2	12 times (30%)	None (0)
Experiment 2	2	3	7 times (17.5%)	Once (2.5%)
Experiment 3	1	4	2 times (5%)	3 times (7.5%)

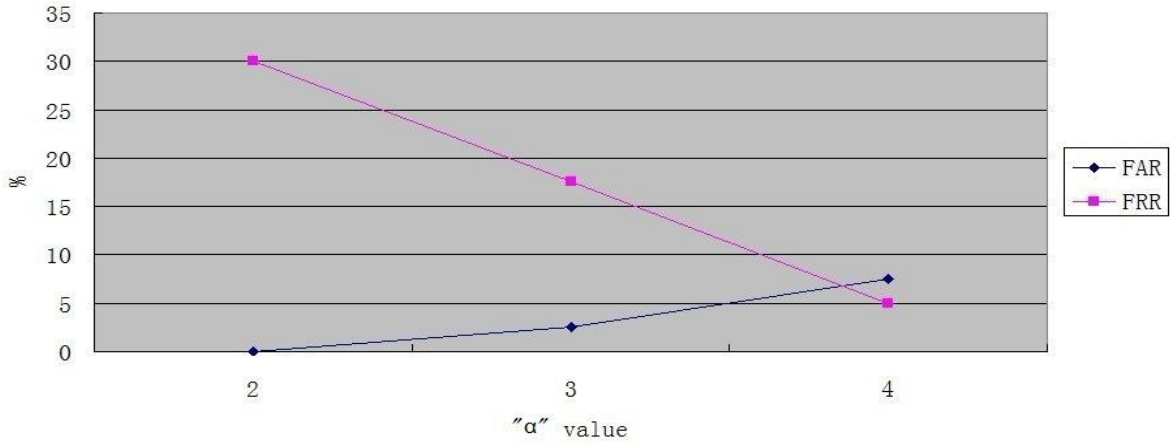

Figure 5. The FAR and FRR in typing recognition experiment

7.5% and it is the best way for the system to achieve the balance between false rejection and false acceptance.

D. Evalution

In terms of this paper, there are two system models can be build according to the result we gained. The first one is multi-level authentication model. In this model, the "α" value can be setup according to different transaction value. For example, when a user wants to buy a newspaper for 50 pence, the "α" value in the system can be setup to 4 or higher to reduce the FRR; if he wants to make some high value transaction like buy a four hundred pounds television, the "α" value can be setup to 3 or lower to improve the authentication rate. This model is suitable to be used in any mobile-commerce system. And the second model can be used in a multi-model biometric authentication system. When typing behaviour recognition technique combines with other biometric techniques, the "α" value in the model can be fixed at 3.8 which can help the system to achieve a better balance between security and usability. The comparisons of the system proposed in this paper and related authentication work is shown in table 3.

Table 3 illustrates the proposed keystroke-based identification system can achieve 7.5% error rate. And in addition to this, the system also defines four security levels which are suitable for the mobile commerce. On the client side, it is simply to implement on most smart phones. From the above descriptions, it can be concluded that the proposed system is effective, secure and convenient for mobile authentication.

IV. CONCLUSIONS AND FUTURE WORK

In this paper, the presented system builds a multi-level mobile authentication model, and also combines with the keystroke analysis technique which can effectively prevent the potential attacks from criminals. The typing behaviour recognition enhances username and password based authentication with keystroke analysis that periodically asks the user to re-verify their identity. In the future, we can use voice and face recognition to provide more accurate and transparent authentication to improve the security of system and reduce the risk. We have a confidence even if the criminals steal or capture user's password but their biometric pattern can not be imitated, it will be difficult to

TABLE III. COMPARISON OF RELATED WORK

Techniques	Authentication systems				
	Zahid et al. (2009)[8]	Campisi et al. (2009)[9]	Sevasti et al. (2009)[10]	Clarke et al. (2007)[2]	Ours
Mobile device	No	Yes	No	Yes	Yes
Keyboard style	Not specified	Numeric	Thumb	Numeric	Full size
Authentication levels	No	No	No	No	Yes
Experimental dataset size	25	25	50	32	40
Error rates (FRR/FAR or ERR)	2%/5.6 %(FRR/FAR)	14.46%	12.2%	12.8%	7.5%

attack the system.

Overview the development status of personal identity recognition techniques, the traditional password-based authentication mechanism has exist a long times in history and currently, it is the most popular mechanism in security area. However, biometric authentication will become the main technology in the future time, but it needs a long time to use biometric authentication mechanism instead of password. At present, individual biometric techniques such as face recognition, voice recognition and typing behaviour recognition can provide valuable enhancements in certain contexts, but are not suited to all users and scenarios. The next step work will focus on build a multi-model biometric authentication system. Perhaps few years later, we can face such a scene: the password-based technology has been completely eliminated, voice recognition, face recognition or another biometric techniques become a global common standards, personal identity recognition will be convenient and secure.

REFERENCES

[1]A.K. Jain, "An introduction to biometric recognition," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, 2004.

[2]N.L. Clarke, S.M. Furnell, "Advanced user authentication for mobile devices," Journal of Computer &Security 26, pp.109-119, 2007.

[3]N. Henze, E. Rukzio, S. Boll. "Observational and experimental investigation of typing behavior using virtual keyboards for mobile devices". Conditionally accepted for CHI 2012 (ACM). 2012.

[4]D.Denning, Information warfare & security. US: ACM Press; 1999.

[5]J. Garcia. "Personal identification apparatus," Patent No. 4 621 334, U.S. Patent and Trademark Office, 1986

[6]S. Blender and H. Postley. "Key sequence rhythm recognition system and method." Patent No. 7 206 938, U.S. Patent and Trademark Office, 2007.

[7]H. Crawford, "Keystroke Dynamics: Characteristics and Opportunities," 2010 Eighth annual international conference on privacy, security and trust. 2010 IEEE, pp 205-213.

[8]L. Araujo, L. S. Jr., M. Lizarraga, L. L. Ling, and J. B. YabuUti, "User Authentication Through Typing Biometrics Features," IEEE Transactions on Signal Processing, vol. 53, Issue 2, Part 2, pp. 851–855, 2005.

[9]S. Zahid, M. Shahzad, S.A. Khayam, and M. Farooq. "Keystroke-Based User Identification on Smart Phones," RAID '09 Proceedings of the 12th International Symposium on Recent Advances in Intrusion Detection Springer-Verlag Berlin, Heidelberg, 2009.

[10]P. Campisi, E. Maiorana, M. L. Bosco, and A. Neri, "User Authentication Using Keystroke Dynamics for Cellular Phones," IET Signal Processing - Special Issue on Biometric Recognition, vol. 3, no. 4, pp.333–341, 2009.

[11]S. Karatzouni and N.L Clarke, "Keystroke Analysis for Thumb-based Keyboards on Mobile Devices," IFIP International Federation for Information Processing, 2007, Volume 232/2007, 253-263.