KEYSTROKE DYNAMIC AUTHENTICATION IN MOBILE CLOUD COMPUTING

MAHNOUSH BABAEIZADEH

A dissertation submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JANUARY 2014

This dissertation is dedicated to my family for their endless support and encouragement.

ACKNOWLEDGEMENT

First and foremost, I would like to express heartfelt gratitude to my supervisors Prof. Dr. Mohd Aizaini Maarof and Dr. Majid Bakhtiari for his constant support during my study at UTM. He inspired me greatly to work in this project. His willingness to motivate me contributed tremendously to our project. I have learned a lot from him and I am fortunate to have him as my mentor and supervisor

Besides, I would like to thank the authority of Universiti Teknologi Malaysia (UTM) for providing me with a good environment and facilities such as Computer laboratory to complete this project with software which I need during process.

ABSTRACT

Contemporary mobile sets are not used just for making calls and sending messages. They are increasingly being used in Mobile Cloud Computing (MCC) to store sensitive and critical information as well as to access sensitive data using the Internet via Cloud Service Provider (CSP). MCC is combination of Cloud Computing (CC) and mobile communication. Using MCC helps to decrease running cost and expansion of mobile applications. One of the important challenges in MCC is security and privacy. Furthermore, authentication plays an important role in preserving security and privacy of shared information in MCC. In fact, the majority of mobile handsets use inherently weak authentication mechanisms, based upon passwords and Personal Identification Number(PINs). But it is not secure way for authenticating users because of its limitation, as well as it is difficult to confirm that the demand is from the rightful owner. This study focus on a type of behavioral biometric authentication that is called Keystroke Dynamic Authentication (KDA) to identify mobile users and improve the authentication mechanism in cloud server. There are different parameters of measuring keystrokes, we defined keystrokes duration as an attribute to identify user. For implementing this method, we use Android SDK development. It includes mobile device emulator, Android Virtual Device (AVD) that helps to develop and test Android applications without using a physical device. Test of the the application is based on three different approaches (client side, local server, cloud server).In the first approach, experimental results is obtained from mobile device (client side) shows that this method works 94% correctly. In the second approach, application is connected to the php server and obtained results show that the application can works 96.15%correctly. In the last approach, obtained results from cloud server (google drive) show that the application can work 95.34% correctly. The important point in these approaches is that, the username and password were known for people cooperate in testing the proposed application. In addition, KDA is based on unique characteristics of users (here keystrokes duration) and it is hard to pretend as legible user. Therefore, applying KDA in mobile set helps to improve security and privacy of authentication.

ABSTRAK

Kontemporari set mudah alih tidak digunakan hanya untuk membuat panggilan dan menghantar mesej. Mereka semakin digunakan di Mobile Cloud Computing (MCC) untuk menyimpan maklumat sensitif dan kritikal serta untuk mengakses data sensitif menggunakan Internet melalui Pembekal Perkhidmatan Awan (CSP) . MCC adalah gabungan Awan Pengkomputeran (CC) dan komunikasi mudah alih. Menggunakan MCC membantu untuk mengurangkan kos menjalankan dan perkembangan aplikasi mudah alih. Salah satu cabaran penting dalam daerah adalah keselamatan dan privasi. Tambahan pula , pengesahan memainkan peranan penting dalam memelihara keselamatan dan privasi maklumat yang dikongsi di MCC . Malah , majoriti telefon bimbit menggunakan mekanisme pengesahan memang lemah , berdasarkan kata laluan dan peribadi Nombor Pengenalan (PIN). Tetapi ia bukan cara yang selamat bagi mengesahkan para pengguna kerana had , dan juga kerana ia adalah sukar untuk mengesahkan bahawa permintaan adalah dari pemilik yang sah . Fokus kajian ke atas jenis pengesahan biometrik tingkah laku yang dipanggil keystroke Dynamic Pengesahan (KDA) untuk mengenal pasti pengguna mudah alih dan meningkatkan mekanisme pengesahan dalam pelayan awan . Terdapat parameter yang berbeza mengukur ketukan kekunci, kita ditakrifkan tempoh ketukan kekunci sebagai sifat untuk mengenal pasti pengguna . Untuk melaksanakan kaedah ini , kami menggunakan pembangunan SDK Android. Ia termasuk mudah alih emulator peranti, Device Maya Android (AVD) yang membantu untuk membangunkan dan ujian Android aplikasi tanpa menggunakan peranti fizikal. Ujian permohonan itu adalah berdasarkan tiga pendekatan yang berbeza (sebelah pelanggan , pelayan tempatan, pelayan awan). Dalam pendekatan pertama, Keputusan eksperimen diperolehi daripada peranti mudah alih (sebelah pelanggan) menunjukkan bahawa ini kaedah kerja-kerja.

TABLE OF CONTENTS

LIST OF TABLES

TABLE OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

The Cloud Computing (CC) became widespread from the 1997 year. The main purpose of CC is providing services via the Internet. CC is a computing method, where a large group of systems are associated with public or private networks.In this case, users able to store their data on Cloud Service Provider (CSP) and access the data on it, everywhere and anytime they need shared information.

Public clouds offer services that are available wherever the end user might be located. This approach cause to easy access to information and accommodates the needs of users in different time and locations. Private Cloud use for a specific group or organization. Shared data in private cloud are accessible to just that group. Private clouds can also support a hybrid cloud model by supplementing local infrastructure with computing capacity from an external public cloud (Sotomayor *et al.*, 2009; Zissis and Lekkas, 2012).

CC has some benefits by permitting users to use infrastructure, platforms, and software provided by CSP. One of the advantage of using CC is reducing the costs for installing softwares as well as hardware. Another advantage is that, you no more have to support the infrastructure. In this case, no need to have the knowledge to develop and maintain the infrastructure.

The expression Mobile Cloud Computing (MCC) was develop no longer after the cloud computing. The research on MCC was start from middle of 2007 year. Using MCC cause to decrease running cost and expansion of mobile applications.

In this case, mobile users can access to the different type of mobile application and services with the lower price. MCC is combination of cloud computing and mobile communication. It helps to mobile's users to utilize variety software, data, applications,infrastructure and services via the Internet.

MCC is an infrastructure which processing of data occurs outside the domain of mobile set. Mobile cloud applications transfer the data storage and computing power from mobile sets to the CSP. In this case, the procedure of processing data is getting more faster.

In addition, mobile cloud applications bring mobile computing and applications to not just user's mobile set but a much broader range of mobile subscribers. Therefore, the mobile devices do not require a powerful conformation (for example, memory capacity and CPU speed) since all the complicated processing and storing the information in memory can be processed in the cloud services.

On the other hand, mobile handsets have found an important place in modern society, with hundreds of millions currently in use. Therefore, authentication plays an important role in preserving security and privacy. It helps to protect mobile systems and shared information from unauthorized persons. An authentication mechanism determines how user identified and verified to access to sensitive information (Altinkemer and Wang, 2011).

Verification of user's identity is the most important goal behind an authentication. Personal identification number (PIN) is often adopted as the only security mechanism for mobile devices. It is obvious that, PIN is not very secure mechanism for authenticating users because of its limitation, as well as it is difficult to confirm that the demand is from the rightful owner (Altinkemer and Wang, 2011).

Strong method of authentication should cover one or several various factors of identification to improve security. These factors are something user know; something user have; something user are. Therefore, biometric authentication (Bhattacharyya *et al.*, 2009; Karnan *et al.*, 2011) is a strong authentication mechanism by providing the factor what we are and what we know (Giot *et al.*, 2009). In addition, it is based on a unique characteristic of a person (Araujo *et al.*, 2005), and it is more reliable, because it is so difficult for user to pretend as other user by using physical or behavioral biometric authentication.

1.2 Problem Background

MCC has a direct relationship with CC. Therefore, all the security issues in CC can be use in MCC. However, these security services should have an additional limitation of resource constraint mobile devices. Hence, it requires lightweight secure structure. In addition, MCC should provide privacy and security with lowest amount of processing and communication. Figure 1.1 shows the different security services that may run on different layers to supply a secure mobile cloud computing environment.

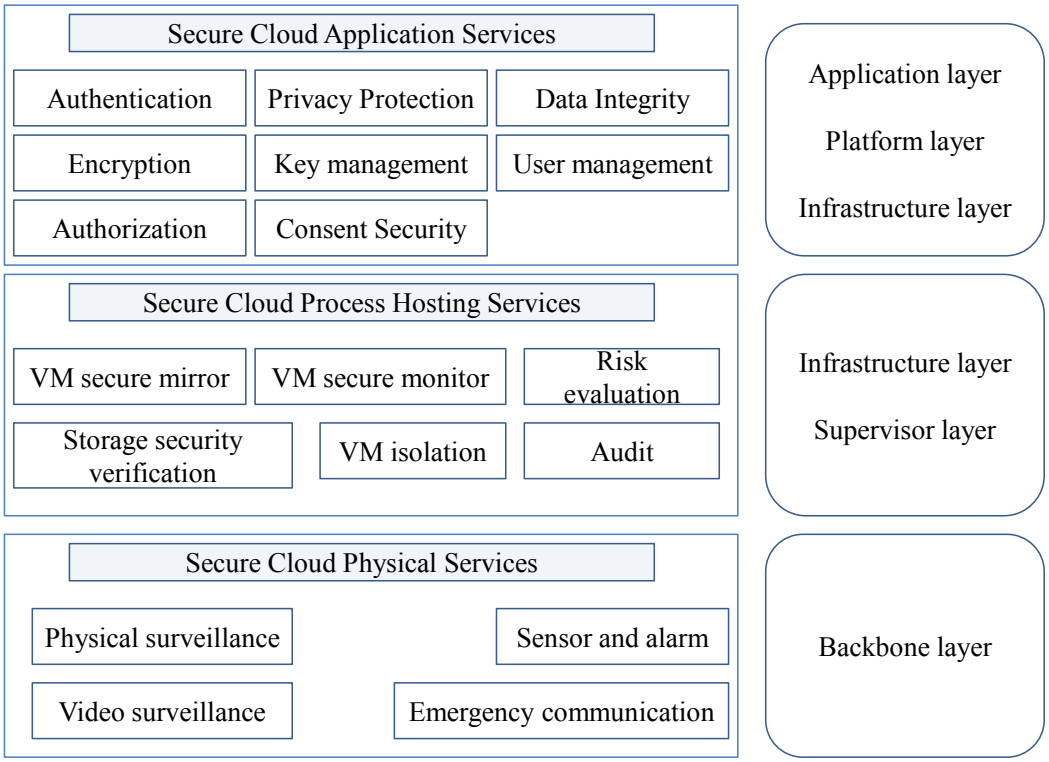

Figure 1.1: Security services on MCC (Khan *et al.*, 2012)

One of the important points in MCC is relate to, providing secure and trustable communication channel among mobile device and CSP. The physical security of the data center has an essential role to achieve privacy and security of user's information.

The main aim of physical security is to keep away from unauthorized people to physically accessing the resources of the cloud service supplier and improve the security and privacy of shared information. Another way to increase the security of communication channel among mobile set and cloud services is using secure routing

protocols to protect the communication channel.

MCC is the combinations of two different fields' mobile network and cloud computing. In this case mobile cloud computing faces many technical challenges. These challenges are categoried as two important folds as following:

1.2.1 Challenges in Mobile Communication

There are some fundamental issues in mobile communication that are as following:

i. Low Bandwidth

It is one of the necessary issues in MCC. One way to impede low bandwidth is to share the restricted bandwidth between mobile users who are involved in the same content and located in the same area.

ii. Availability

It means CSP should be available at all time and every where the mobile users requested to access the services. Mobile users may not be capable to communicate with the CSP due to network failures, traffic congestion, and the out-of-signal. Therefore, they can communicate with the cloud services through their neighboring nodes, as an alternative, having a direct effective on the cloud. Also, each node regularly broadcasts control messages to notify other nodes of its new local content and status.

1.2.2 Issues in Computing Side

There are three fundamental issues in mobile communication that are as following:

i. Computing Offloading Computing offloading is transport data, software, application locally by using network. This way has some advantages such as the availability of higher bandwidth and cost control. More over, offloading apply to modify the battery lifetime for the mobile procedure and to enhance the

performance of applications. Also, it can categories to two types offloading in the static environment and offloading in the dynamic environment.

ii. Protecting Privacy and Security Protecting data secrecy and user privacy play crucial role to preserve user's trust in the mobile technology, especially in MCC (Jeong and Choi, 2012). These issues are in three types security of mobile users, security and privacy of mobile applications, as well as privacy (Corapi *et al.*, 2010).

1.2.3 Privacy of Authentication in MCC

One of the most challenges in MCC related to authentication (Nauman *et al.*, 2011). There is increasing demand for suitable authentication method to access services, application, and data for both consumers and enterprisers. There are several authentication schemes that we can classify them in three folds something the user knows, something the user has, something the user is.

Password can be observed, forgotten, or shared. Moreover, in electronic world people should remember a multitude of Personal Identification Number (PIN) and passwords for e-mail, security code of phone, computer accounts, as well as Automated Teller Machine (ATM). Therefore, it is so difficult to memories all these passwords. Biometric authentication methods are not face with these issues. It holds the promise of accurate, fast, less expensive, reliable authentication for a difference applications (Bhattacharyya *et al.*, 2009).

Biometric authentication is applied to recognize the characteristics of an input sample compare with a template, employ in cases to identify specific people by particular characteristics. It can categories in two types, physiological characteristics, and behavioral characteristics. Physiological biometrics relies on *something the users are*. It performs authentication based on physical characteristics such as retinal scan, face recognition, and fingerprint. By contrast, behavioral biometrics perform authentication based on the way people do things, such as typing rhythm, voice and signatured (Bhattacharyya *et al.*, 2009).

Keystroke authentication is a type of behavioral biometric authentication. Keystroke based authentication can categorize in two folds, Keystroke Static Authentication (KSA), as well as Keystroke Dynamic Authentication (KDA).

Keystroke static authentication can identify keystroke of users only at particular times, for example the time that user wants to login. This is a huge draw back as anyone can then use the system once the user is authenticated at login (Choras and Mroczkowski, 2007).

KDA continuously observes the style of typing of the users throughout the whole stage of interaction even after a successful login. In the other words, the typing patterns of users are constantly analyzed and when they do not match accessing of users will block (Bhatt and Santhanam, 2013; Teh *et al.*, 2013).

One of the first researches on keyboard biometrics was carried out by (Gaines *et al.*, 1980). Seven secretaries took part in the experiment in which they were asked to retype the same three paragraphs on two different occasions in a period of four months. Keystroke latency timings were collected and analyzed for a limited number of digraphs and observations were based on those digraph values that occurred more than 10 times.

Base on study of (Clarke and Furnell, 2007), keystroke based authentication is not suitable for all users, specifically types of user with large changes in their handset interactions. Also, this technique will not be suitable for users who do not regularly use their mobile handset and in particular.

Keystroke based authentication can categories in two important folds, static and dynamic. Static keystroke analysis is performed on typing samples produced using predetermined text for all the individuals under observation. Dynamic analysis implies a continuous or periodic monitoring of issued keystrokes. It is performed during the log-in session and continues after the session (Karnan *et al.*, 2011).

Keystroke dynamics is a behavioral measurement and it aims to identify users based on the typing of the individuals or attributes such as force of keystrokes, key hold time, latency of keystrokes, typing error, etc.

Keystroke dynamic authenticate has some advantages over other biometric authentication methods as following:

i. Majority of biometrics-based mechanisms require an additional device to authenticate user, however KDA requires no extra device.

ii. The mechanism of this type of authentication no need any further inconvenience to do by user.It means that the process of login is easy.

iii. Scanned iris or fingerprint needs a large space of memory, a higher computing power than keystroke timing vectors.

iv. The effectiveness of KDA is very significant in mobile communication which attends to have a lower computing power,smaller memory.

v. KDA can help to improve privacy and security of mobile cloud computing.

1.3 Problem Statement

Mobile handsets have found an important place in modern society, with hundreds of millions currently in use. The majority of these devices use inherently weak authentication mechanisms, based upon passwords and Personal Identification Number(PINs). But it is not secure way for authenticating users because of its limitation, as well as it is difficult to confirm that the demand is from the rightful owner. This study focus on a type of behavioral biometric authentication that is called Keystroke Dynamic Authentication (KDA) to identify mobile users and improve the authentication mechanism in MCC.

The sub-questions of using KDA in MCC are as following:

- How to trust on the pattern of user's keystroke reported by the client side (mobile set) ?
- How to measure keystrokes of mobile's user?
- What is the advantage of using KDA in MCC?
- How to extend KDA to improve security and privacy of user authentication in MCC?
- How to create the secure communication between mobile user and cloud servers?

1.4 Purpose of Research

The purpose of this research is, developing an android application. This application is able to authenticate mobile users based on KDA authentication. There are different parameters for measuring keystrokes of users in MCC. In this study, we defined keystrokes duration as an attributes to measuring keystrokes of mobile users in MCC. In other words, the proposed application is able to authenticate mobile users based on measuring their keystroke duration. Applying KDA in MCC cause to to improve the security and privacy of authentication mechanism in MCC.

1.5 Objectives

The main objectives of this research are as following:

i. To study and analyze the current method of authentication in MCC.
ii. To design the keystroke dynamic confirmation in MCC.
iii. To implement and test the method of authentication in MCC by using KDA.

1.6 Scope of the Project

The scope of this research includes:

i. Applying KDA in MCC.
ii. Android SDK for developing the proposed android application.
iii. Keystrokes duration as an attributes for verification of mobile's user.

1.7 Significant of Study

The main goal of this thesis is, development android application which able to identify users based on keystrokes authenticate mechanism in MCC. This method of authentication is based on their unique characteristics (typing manner of users). In

this study, keystrokes duration is defined as an attributes to identify users. Because keystrokes duration is relate to the behavioral characteristics of users, it is so difficult for attackers to pretend as user. Therefore, the proposed application helps to improve the security and privacy of authentication in MCC.

1.8 Organization of Project

This thesis is organized into five chapters the content of each chapter is presented as following: Some review on MCC and discussing about different issues in this area on Chapter 1. Explanation about different technologies used for authenticate users in MCC, moreover discuss about advantages and disadvantaged of each method, and their subsets in Chapter 2. Research methodology that is based on KDA and improve security of authentication on MCC has explained in Chapter 3, analysis and designing the proposed authentication method is in Chapter4. In addition implementation and test of proposed an android application has been done in Chapter 5. In the last, conclusion has been explained in Chapter 6.

REFERENCES

Abhishek, K., Roshan, S., Kumar, P. and Ranjan, R. (2013). A Comprehensive Study on Multifactor Authentication Schemes. In *Advances in Computing and Information Technology*. (pp. 561–568). Springer.

Altinkemer, K. and Wang, T. (2011). Cost and benefit analysis of authentication systems. *Decision Support Systems*. 51(3), 394–404.

Araujo, L., Jr, L. S., Lizarraga, M., Ling, L. and Yabu-Uti, J. (2005). User authentication through typing biometrics features. *Signal Processing, IEEE Transactions on*. 53(2), 851–855.

Bartlow, N. and Cukic, B. (2006). Evaluating the reliability of credential hardening through keystroke dynamics. In *Software Reliability Engineering, 2006. ISSRE'06. 17th International Symposium on*. IEEE, 117–126.

Bergadano, F., Gunetti, D. and Picardi, C. (2002). User authentication through keystroke dynamics. *ACM Transactions on Information and System Security (TISSEC)*. 5(4), 367–397.

Bhatt, S. and Santhanam, T. (2013). Keystroke dynamics for biometric authenticationA survey. In *Pattern Recognition, Informatics and Medical Engineering (PRIME), 2013 International Conference on*. IEEE, 17–23.

Bhattacharyya, D., Ranjan, R., Farkhod, A. and Choi, M. (2009). Biometric authentication: A review. *International Journal of u-and e-Service, Science and Technology*. 2(3), 13–28.

Card, S., Moran, T. and Newell, A. (1987). Computer text-editing: An information-processing analysis of a routine cognitive skill. In *Human-computer interaction*. Morgan Kaufmann Publishers Inc., 219–240.

Cho, S. and Hwang, S. (2005). Artificial rhythms and cues for keystroke dynamics based authentication. In *Advances in Biometrics*. (pp. 626–632). Springer.

Choras, M. and Mroczkowski, P. (2007). Keystroke dynamics for biometrics identification. In *Adaptive and Natural Computing Algorithms*. (pp. 424–431). Springer.

Clarke, N. and Furnell, S. (2007). Authenticating mobile phone users using keystroke analysis. *International Journal of Information Security*. 6(1), 1–14.

Corapi, D., Russo, A. and Lupu, E. (2010). Inductive logic programming as abductive search. In *26th International Conference on Logic Programming, Leibniz International Proceedings in Informatics. Schloss Dagstuhl Research Online Publication Server*.

Dabbah, M., Woo, W. and Dlay, S. (2007). Secure authentication for face recognition. In *Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on*. IEEE, 121–126.

De, R., Willem, G. and Eloff, J. H. P. (1997). Enhanced password authentication through fuzzy logic. *IEEE Expert*. 12(6), 38–45.

Gaines, R., Lisowski, W., Press, S. and Shapiro, N. (1980). *Authentication by keystroke timing: Some preliminary results*. Technical report. DTIC Document.

Giot, R., El-Abed, M. and Rosenberger, C. (2009). Keystroke dynamics authentication for collaborative systems. In *Collaborative Technologies and Systems, 2009. CTS'09. International Symposium on*. IEEE, 172–179.

Haidar, A. N. and Abdallah, A. E. (2009). Formal modelling of pki based authentication. *Electronic Notes in Theoretical Computer Science*. 235, 55–70.

Hoang, T. D., Chonho, L., Dusit, N. and Ping, W. (2011). A survey of mobile cloud computing: architecture, applications, and approaches. *Wireless Communications and Mobile Computing*. ISSN 1530-8677.

Hong, L. and Jain, A. (1998). Integrating faces and fingerprints for personal identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*. 20(12), 1295–1307.

Hwang, S., Cho, S. and Park, S. (2009). Keystroke dynamics-based authentication for mobile devices. *Computers & Security*. 28(1), 85–93.

Jakobsson, M., Shi, E., Golle, P. and Chow, R. (2009). Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX conference on Hot topics in security*. USENIX Association, 9–9.

Jeong, H. and Choi, E. (2012). User Authentication using Profiling in Mobile Cloud Computing. *AASRI Procedia*. 2, 262–267.

Joyce, R. and Gupta, G. (1990). Identity authentication based on keystroke latencies. *Communications of the ACM*. 33(2), 168–176.

Kang, P., Park, S., Hwang, S., Lee, H. and Cho, S. (2008). Improvement of keystroke data quality through artificial rhythms and cues. *Computers & Security*. 27(1),

3–11.

Karnan, M., Akila, M. and Krishnaraj, N. (2011). Biometric personal authentication using keystroke dynamics: A review. *Applied Soft Computing*. 11(2), 1565–1573.

Khan, A., Kiah, M., Khan, S. U. and Madani, S. A. (2012). Towards secure mobile cloud computing: a survey. *Future Generation Computer Systems*.

Kim, M., Ju, H., Kim, Y., Park, J. and Park, Y. (2010). Design and implementation of mobile trusted module for trusted mobile computing. *Consumer Electronics, IEEE Transactions on*. 56(1), 134–140.

Lin, D. (1997). Computer-access authentication with neural network based keystroke identity verification. In *Neural Networks, 1997., International Conference on*, vol. 1. IEEE, 174–178.

Loy, C., Lai, D. and Lim, D. (2005). Development of a pressure-based typing biometrics user authentication system. *ASEAN Virtual Instrumentation Applications Contest Submission*.

Magalhaes, M., Paulo, S. and Santos, H. D. (2005). An improved statistical keystroke dynamics algorithm.

Mario, C., Penedo, M., Penas, M., Carreira, M. and Gonzalez, F. (2006). Personal authentication using digital retinal images. *Pattern Analysis and Applications*. 9(1), 21–33.

Monrose, F. and Rubin, A. (1997). Authentication via keystroke dynamics. In *Proceedings of the 4th ACM conference on Computer and communications security*. ACM, 48–56.

Monrose, F. and Rubin, A. (2000). Keystroke dynamics as a biometric for authentication. *Future Generation Computer Systems*. 16(4), 351–359.

Nauman, M. and Ali, T. (2010). Token: Trustable keystroke-based authentication for web-based applications on smartphones. In *Information security and assurance*. (pp. 286–297). Springer.

Nauman, M., Ali, T. and Rauf, A. (2011). Using trusted computing for privacy preserving keystroke-based authentication in smartphones. *Telecommunication Systems*, 1–13.

Obaidat, M. S. and Sadoun, B. (1997). Verification of computer users using keystroke dynamics. *Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on*. 27(2), 261–269.

Radha, V. and Reddy, D. H. (2012). A Survey on Single Sign-On Techniques. *Procedia Technology*. 4, 134–139.

Recordon, D. and Reed, D. (2006). OpenID 2.0: a platform for user-centric identity management. In *Proceedings of the second ACM workshop on Digital identity management*. ACM, 11–16.

Robinson, J. A., Liang, V., Chambers, J. M. and MacKenzie, C. L. (1998). Computer user verification using login string keystroke dynamics. *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on*. 28(2), 236–241.

Saevanee, H., Clarke, N. L. and Furnell, S. M. (2012). Multi-modal Behavioural Biometric Authentication for Mobile Devices. In *Information Security and Privacy Research*. (pp. 465–474). Springer.

Shi, E., Niu, Y., Jakobsson, M. and Chow, R. (2011). Implicit authentication through learning user behavior. In *Information Security*. (pp. 99–113). Springer.

Song, Z., Molina, J., Lee, S., Lee, H., Kotani, S. and Masuoka, R. (2009). Trustcube: An infrastructure that builds trust in client. In *Future of Trust in Computing*. (pp. 68–79). Springer.

Sotomayor, B., Montero, R. S., Llorente, I. M. and Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. *Internet Computing, IEEE*. 13(5), 14–22.

Teh, P. S., Teoh, A., Tee, C. and Ong, T. S. (2010). Keystroke dynamics in password authentication enhancement. *Expert Systems with Applications*. 37(12), 8618–8627.

Teh, P. S., Teoh, A. B. J., Tee, C. and Ong, T. S. (2011). A multiple layer fusion approach on keystroke dynamics. *Pattern Analysis and Applications*. 14(1), 23–36.

Teh, P. S., Teoh, B. and Yue, S. (2013). A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal*. 2013.

Tripathi, A. and Mishra, A. (2011). Cloud computing security considerations. In *Signal Processing, Communications and Computing (ICSPCC), 2011 IEEE International Conference on*. IEEE, 1–5.

Wang, X., Fangxia, G. and Jian-feng, M. (2012). User authentication via keystroke dynamics based on difference subspace and slope correlation degree. *Digital Signal Processing*. 22(5), 707–712.

Wood, H. M. (1977). The use of passwords for controlling access to remote computer systems and services. In *Proceedings of the June 13-16, 1977, national computer conference*. ACM, 27–33.

Young, J. R. and Hammon, R. W. (1989). *Method and apparatus for verifying an individual's identity*. US Patent 4,805,222.

Zissis, D. and Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*. 28(3), 583–592.