Volume 6, Issue 2, February 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Rhythm Based Authentication Model: Towards Secure and Convenient Authentication for Mobile Devices

Priyanka Gawali, Prof. V. D. Jadhav
CSE Department, SVERIs COE Pandharpur,
Solapur University, Solapur, Maharashtra, India

Abstract— As we know in today's world, everywhere we are using mobiles only and through mobile only we are doing our work, for example our private data, files ,account, different logins on social websites .So it is very important to provide security to our device. Already we have seen different techniques for providing the security for mobile phones like-password, patterns. The main security problem is user authentication. if we are not going to provide it in correct way, it will be harmful and causes effects like impersonation and unauthorized access for persons own device. Present studies have shown mobile users preferring usability over security. Usually, mobile users unlock their devices in public spaces, which may cause problem like user credentials disclosure. So, we use a paper called rhythm based authentication model, where mobile users can integrate their own habits (or hobbies) with user authentication on mobile devices.

Keywords— Rhythm-based authentication, Sensor Based User Authentication /Identification, Methodology, FAM Based Authentication Algorithm

I. INTRODUCTION

User authentication is crucial to mobile device security, but unfortunately, many studies have shown that mobile users prefer usability over security. Yet, a higher level of security often entails sacrificing usability. As such, most people don't lock their devices at all because of two reasons. Reason one, entering a pass code is inconvenient on a small screen like a mobile phone. Reason two, mobile users are limited to or given no user-friendly options. Motivated by the aforementioned observations, we aim at securing mobile phones in a user-friendly manner by allowing mobile users to authenticate themselves using authentication services combined with their habit since it is likely that the user would prefer to use an authentication scheme that fits their habits.

Some of the recent and most relevant works are summarized below:

In Cisco[1] This paper presents some of Cisco's major global mobile data traffic projections and growth trends. Cigital's [2]mobile experts have helped customers of all types implement a proactive approach to security that helps them find, fix and prevent vulnerabilities in their mobile apps.

N. L. Clarke and S. M. Furnell [3] did Whilst keystroke analysis using mobile devices have been proven effective in experimental studies, these studies have only utilized the mobile device for capturing samples rather than the more computationally challenging task of performing the actual authentication.

M. Jakobsson, E. Shi, P. Golle, and R. Chow, introduces the notion of implicit authentication – the ability to authenticate mobile users based on actions they would carry out anyway. McAfee[6] Smartphone's and tablets offer a unique synthesis of online and mobile lifestyle

II. RELATED WORK

The main purpose in this study is to propose an alternative to users of Smartphone, especially dependent people, different from explicit authentication by using context information, leading to an implicit authentication. In a comparison with the state-of-art in the context-based authentication field, we represent a set of related works already done.

2.1.1 Behavioural User Authentication / Identification

A user behavioural model is provided in [1], the corresponding research is based on the idea that the person is a creature of habit, therefore each event has a correlation between two fundamental attributes: space and time. The proposed architecture uses resources found in the mobile devices: User calls, user schedule, GPS, device battery level, user applications, and sensors. This model is clearly implemented by same authors in [2].

2.1.2. Sensor Based User Authentication /Identification

Researchers proposed SenGuard [5] as a new user identification framework that offers continuous and implicit user identification service for the Smartphone. SenGuard is a new passive authentication technique that leverages the sensors available on the Smartphone. It uses four sensors: voice, multitouch, locomotion and location. These sensors are processed together in order to get the user identification features implicitly, explicit authentication is performed only when there is an important evidence that the user has changed.

2.1.3 Biometric Based Authentication

Biometric based authentication is an important alternative for explicit authentication. However, according to the limitations in the size, power efficiency, and mainly the cost of a smart phone, the usage of physiological features on a mobile are less attractive and researchers omitted the emergence on these kinds of recognition in a Smart phone. Several studies experimented user authentication/ identification using gait recognition as a possible implicit authentication method. The proposed approach uses acceleration signal and detects the person's way of walking [6]. A motion-recording device was used [7], [8] in order to measure the acceleration according to the three axes, there were multiple algorithm proposed including histogram similarity, and cycle length measurement techniques.

III. METHODOLOGY

The proposed scheme consists of two phases: Registration and Authentication, as shown in Figure.

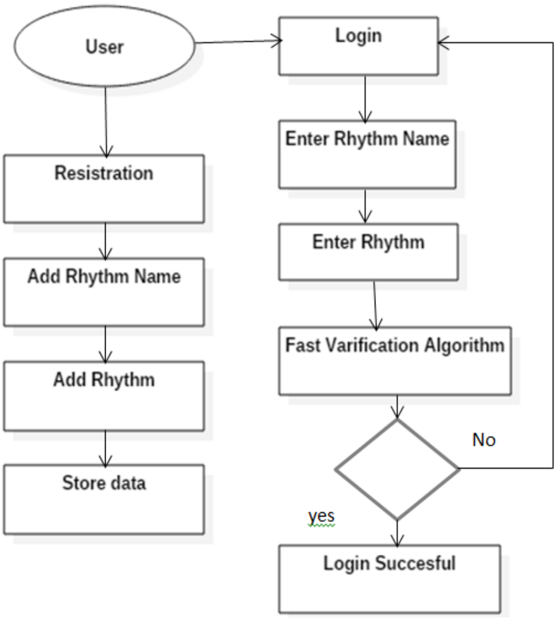

Fig 1: Data flow Diagram

Original Data Acquisition

The accelerometer is one kind of common hardware sensors used to capture a users' shake motion. In most smart phones, the accelerometer adopts a standard 3-axis coordinate system that is denoted relative to the device's screen and expresses them as data values.

Fast Verification Algorithm

The registration process is performed during a user's initial log on. A well-designed authentication scheme is required to have a user-friendly registration process with less user operations, which is the key factor that impact the user's experience. Due to human cognitive behaviour variance and input errors, it is very difficult for most users to input the same rhythms twice as opposed to traditional authentication schemes like password or grid pattern. We propose a fast verification algorithm, by which user only needs to use two similar rhythms (the first one for template setting and the second one for verification) to complete the registration process with adjustable precision level. Moreover, the proposed fast verification algorithm is also in charge of providing effective sample data for the training of the FAM system in the authenticate phase. It can be observed that the captured original data consists of not only the rhythm input, but also the noise due to unstable Smartphone holding. In addition, due to the sampling precision, the accelerometer maybe too sensitive in terms of capturing both rhythm's amplitude and duration (in milliseconds) between the first initial input and second confirmation input. We may have two relatively different signals because of this, when in fact, they are the same rhythm entered by the same user. To avoid false positives, the proposed fast verification algorithm includes a threshold comparison approach that transforms the original data to the binary data, aiming at reducing the noise and the randomness of signal amplitude; and three techniques, named zero-shrinkage, threshold matching and e-error correction, to control the tolerable precision between two consecutive samples.

a. Data Transformation

To reduce the uncertainty of the amplitude (due to the tapping speed), we first transform the original data from the real number S(n) to the binary data BTemplate(n) by using a comparison threshold method. When the beat of a rhythm peak beyond the threshold, whether it is larger or smaller, it will be labelled as 1. Otherwise, it will be labelled as 0.when we tap a rhythm on different points, the acceleration values on the three axis work differently, and therefore, we need to specify the threshold based on the merits. Particularly, when Point A and Point B are used.

b. Zero-Shrinkage

Using data transformation, we obtain the binary data BTemplate consisting of two alternating symbols ``0" and ``1",where ``0" represents the idle time waiting for input, and ``1" refers to the rhythm user input. The time interval between two symbols is 1=Fs seconds. In order to control the precision level while maintaining useful information, we design a zero-shrinkage approach that

reduces the number of symbols ``0" in proportion but keeps ``1" unchanged shrinkage, where [.] is the rounding operation.

c. Threshold Matching

In the verification and the following stages, as the template information have been obtained, we can relax the constraint of fixed threshold by using an adaptive threshold matching approach, thereby further lowering the number of times the user is required to input during the training stage. we can see that when user enters a beat from Point A, a positive impulse appears, which usually distributes on the relatively fixed interval (positive impulse In addition, a positive impulse is immediately followed by a negative impulse because of counter acting force of holding hand. Utilizing these features, we can search a more proper threshold in case the tapping motions are unstable.

d. e-ERROR Correction

This is an additional precision control process used for the verification and authentication input. Denote the number of symbols ``0" between any two consecutive ``1" of BZS Template and BZS Verification be ZZS Template(k) and ZZS Verification(k), respectively, where 1<= k <= N -1,then input ZZS Verification is considered similar to the rhythm template, where scalar e is the correction factor that can be adjusted.

IV. FAM BASED AUTHENTICATION ALGORITHM:

In this subsection, we propose an FAM-based authentication algorithm to further improve the performance of the rhythm authentication scheme. Compared with the fast authentication algorithm, the advantages of the FAM-based algorithm are four-folds:

(1) it is independent on the algorithm parameters, such as d and e in the fast authentication algorithm, which makes the proposed authentication scheme more flexible for different users.

(2) by means of the extendibility feature of the FAM system, it is easy to extend the proposed authentication scheme for more application scenarios, like multiuser authentication.

(3) more characteristics of the rhythm input might be utilized as the input of the FAM system, to further improve the security and accuracy of the proposed authentication scheme; and

(4) a well-trained FAM system performs better in terms of computation complexity.Review on Fuzzy ARTMAP: FAM is an extension of ARTMAP neural network that perform incremental supervised learning of recognition categories and multidimensional maps in response to input vectors (analog or binary) presented in arbitrary order.

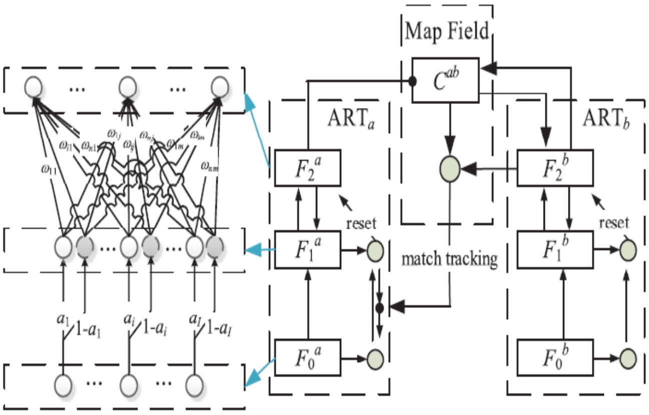

Fig 2.The structure of FAM.

i) Training

In this stage, ARTa receives a stream of training rhythm patterns that was verified by the fast verification algorithm, and the normalization of

(N -1) dimensional ZAuthentication, where **1** is (N - 1)-dimensional vector with all elements of 1 and Dmax is the predefined maximal interval between two consecutive rhythm.

ii) Authentication

After training, the FAM network can be used to verify the given input data with the specified vigilance parameter. Specifically, when a new authentication data is received and processed by threshold matching, we first check if Matching = N is satisfied.

iii) Music Confirmation

We further provide an optional authentication step, ``Music Confirmation'', for some security-aware users or in an insecure environment (e.g. public area). The optional step is able to increase the security of our proposed scheme significantly, while at little expense of user experience. When the input rhythm passed the proposed verification algorithm, a question page appears to ask the user to type the name of the music just input. Obviously, a legitimate user would be easy to answer what he/she has tapped is. However, it will be very difficult for attackers to guess the connection between the observed tapping motions and the corresponding music.

V. CONCLUSION

In this paper, we have presented rhythm based authentication scheme,which is a user-friendly.In this paper mobile users are going to use none other than their own habits as we have defined earlier for giving authentication to their mobiles in terms of security.The proposed scheme satisfies requirement user friendliness into an enjoyable actions.The experimental results shows that it has high accuracy in terms of false rejection rate.As well as it is helpful for multiple user login/registration.

REFERENCES

[1] Cisco. (Feb. 2014). Cisco Visual Networking Index: Global Mobile Data Traf_c Forecast Update, 2013_2018..

[2] A. Sethi, O. Manzoor, and T. Sethi, User Authentication on Mobile Devices,Cigital, Dulles, VA, USA, 2012.

[3] N. L. Clarke and S. M. Furnell, ``Authenticating mobile phone users using keystroke analysis,'' Int. J. Inf. Secur., vol. 6, no. 1, pp. 1_14, Jan. 2007.

[4] S. Furnell, N. Clarke, and S. Karatzouni, ``Beyond the PIN: Enhancing user authentication for mobile devices,'' Comput. Fraud Secur., vol. 2008, no. 8,pp. 12_17, Aug. 2008.

[5] M. Jakobsson, E. Shi, P. Golle, and R. Chow, ``Implicit authentication for mobile devices,'' in Proc. 4th USENIX Conf. Hot Topics Secur. (HotSec),2009, pp. 9_15.

[6] McAfee.(Feb.2014).Who's Watching You?http://www.mcafee.com/ca/resources/reports/rp-mobile-security-consumer-trends.pdf .

[7] D. Drinkwater. (Feb. 2014). RSA 2014: Touchlogging the New Attack Vector for Mobile Hackers.

[8] J. Seto, Y. Wang, and X. Lin,``Toward secure user-habit-oriented authentication for mobile devices,'' in Proc. IEEE Int. Conf. Global Commun. (GLOBECOM), Dec.2014, pp. 1242_1248.

[9] Has the iPhone 5S Fingerprint Scanner Already Been Hacked ?fingerprint scanner-already-been-hacked-1.1468316, accessed Dec. 12, 2014.

[10] R. A. Dora, P. D. Schalk, J. E. McCarthy, and S. A. Young, ``Remote suspect identification and the impact of demographic features on keystroke.