Smart Kiosk with Gait-Based Continuous Authentication

Duong-Tien Phan(✉), Nhan Nguyen-Trong Dam,
Minh-Phuc Nguyen, Minh-Triet Tran, and Toan-Thinh Truong

Faculty of Information Technology, University of Science VNU-HCM,
Ho Chi Minh City, Vietnam
dntnhan@apcs.vn, {1112328,1112224}@student.hcmus.edu.vn, {tmtriet,ttthinh}@fit.hcmus.edu.vn

Abstract. The authors propose to develop a smart kiosk that plays the role of an identity selector activated implicitly when a user is approaching that kiosk. The identity of a user is recognized implicitly in background by a mobile/wearable device based on his or her gait features. Upon arriving at a smart kiosk, the authentication process is performed automatically with the current available user identity in his or her portable device. To realize our system, we propose a new secure authentication scheme compatible with gait-based continuous authentication that can resist against known attacks, including three-factor attacks. Furthermore, we also propose a method to recognize users from their moving patterns using multiple SVM classifiers. Experiments with a dataset with 38 people show that this method can achieve the accuracy up to 92.028 %.

Keywords: Gait-based recognition · Continuous authentication · Smart kiosk · Mobile device · Wearable device

1 Introduction

Ambient intelligence allows the creation of smart interactive environments in which users can access useful data and services fitting their own demand at anytime and anywhere. Upon recognizing a user's identity, a computing system can provide appropriate features and services. Therefore, authentication is one of the essential steps for smart interactive environments.

In this paper, we propose an architecture for a Smart Kiosk system. A smart kiosk plays the role of an identity selector activated implicitly when a user is approaching that kiosk. By this way, when a user arrives at an available kiosk in idle state, i.e. there is no active user using that kiosk, the kiosk allows that user to access various online services, such as Facebook, Gmail, Flickr, etc. with appropriate identities associated with his or her registered account in Smart Kiosk system. With a flexible architecture, new types of services can be integrated into a smart kiosk.

We choose gait feature as a biometric factor and design a compatible scheme for our proposed Smart Kiosk system. Our system exploits gait features, body movement patterns of a user, for implicitly continuous user identification and authentication.

© Springer International Publishing Switzerland 2015
N. Streitz and P. Markopoulos (Eds.): DAPI 2015, LNCS 9189, pp. 188–200, 2015.
DOI: 10.1007/978-3-319-20804-6_18

By this way, a user can access not only utilities in a kiosk but also other online services, such as Facebook, Gmail, Flickr, etc. at kiosks available in public areas.

User's gait dominates the security of the system. Using gait-based authentication allows us to avoid the vulnerability when traditional authentication tokens, such as active badge with infrared signal, RFID tags, or NFC-enable tokens are lost or stolen. Furthermore, as the authentication process is carried out in background continuously, it would be more natural for users to access their data and services immediately without performing an explicit authentication step, such as pushing fingers into a fingerprint scanner, or speaking to a microphone.

There are two main components in our proposed Smart Kiosk system: (i) gait-based continuous authentication module in a wearable device/mobile device, and (ii) interactive kiosk to provide users with services corresponding to their identities.

The main contributions of our papers are as follows:

- We study and analyze the security of biometric-based scheme by Khan et al. [5] and show that the scheme still cannot resist three-factor attacks. We then propose a new scheme to fix this vulnerability. By this way, we stress the importance of biometric factor, which does not have a discernible interest.
- We propose a new method for implicitly continuous gait-based authentication embedded in a wearable/mobile device. In our proposed method, we use multiple SVM classifiers to boost the accuracy for user identity classification from gait data captured from motion sensors of a wearable/mobile device.

The structure of our paper is as follows. In Sect. 2, we first introduce the notations used for authentication schemes in this paper and present the advantages and vulnerability of existing secured authentication schemes, especially against three-factor attacks. We then present the trend to apply biometric features for authentication to replace traditional approaches and several existing methods for gait-based identity recognition. In Sect. 3, we present our proposed Smart Kiosk system with continuous implicit gait-based authentication via mobile/wearable devices. The details of our proposed authentication scheme using biometric features (i.e. gait features) and our method to recognize a user based on his or her gait feature using multiple SVM classifiers are presented in Sect. 4. Section 5 focuses on security analysis of our proposed authentication scheme as well as experimental results to evaluate the accuracy of gait-based identity recognition. Conclusions and discussion on future work are in Sect. 5.

2 Background and Related Work

2.1 Secured Authentication Scheme

Traditional authentication is based on passwords [1] and is susceptible to dictionary attacks. To improve security, two-factor [2, 3] and three-factor [4–7] authentication schemes have been proposed. In 2012, An proposed an enhancement of an efficient biometrics-based remote user authentication scheme using smart cards [4], and claimed that the scheme was secure against many kinds of attack, such as user impersonation

attack, server masquerading attack. In 2013, Khan et al. [5] showed that An's scheme was vulnerable to several attacks and could not provide mutual authentication between the user and the server. In order to fix the flaws, Khan et al. proposed their improved scheme and claimed that the new scheme was secure even if the secret information stored in the smart card was revealed to an attacker. With this concern, Khan et al. have a further step in the right direction that is protecting user even though more and more information is leaked. In 2014, Sarvabhatla et al. [6] and Wen et al. [7] respectively analyzed the weakness of Khan et al.'s scheme, such as off-line password guessing attack, impersonation attack, server masquerading attack, malicious user, stolen smart card, leakage of password, parallel session attack. They both proposed new biometrics-based scheme and claimed that the schemes was secure and resisted all major cryptographic attacks.

However, Sarvabhatla et al. and Wen et al. do not consider the use of biometric factor in Khan et al.'s scheme. We point out that Khan et al.'s scheme cannot take the advantage of biometric factor. As a result, this scheme is vulnerable to three-factor attacks. This kind of attack implies that attacker has two of the three factors: password, shared information, and biometric [8]. In biometrics-based scheme, users should be safe even when password and shared information are leaked. Moreover, user's identity should be kept secret in the scheme, but it can still protect a user when ID is leaked.

Our new scheme utilizes biometrics as the main security factor to fix the vulnerability in Khan et al.'s scheme. We also employ the strategy in our previous work [9, 10] to use random numbers and hash functions to establish a secure authentication process with multi servers using mobile or wearable devices.This strategy requires less computation cost than methods with bi-linear pairing.

2.2 Cryptanalysis Khan et al.'s Scheme

For simplicity of presentation, we introduce the main notations used in authentication schemes presented in this paper. We inherit these notations from the scheme by Khan et al. [5] (Table 1).

In Khan et al.'s scheme, the value $g_i = (ID_i||PW_i) \oplus f_i$ is stored in the smart card. Note that, the value $f_i = h(B_i \oplus K_i)$ is biometric factor in this scheme. An attacker can retrieve f_i easily by computing $(ID_i||PW_i) \oplus g_i$. Therefore, the security of this scheme is downgraded by perform three-factor attack and biometric factor have no advanced.

Table 1. Notations with their descriptions

Notations	Description	Notations	Description
R	Trusted registration center	K_i	Random number chosen by U_i
S_i	Server	R_c	Random number generated by SC_i
U_i	i^{th} user	R_s	Random number generated by S_i
ID_i	Identity of U_i	x_s *and* y_s	Secret keys maintained by S_i
PW_i	Password of U_i	$h(.)$	One-way hash function
B_i	Biometric template of U_i	$\oplus$	Bitwise XOR operator
SC_i	Smart card of U_i	$\|\|$	Concatenation operator

In order to perform three-factor attack, we assume attacker have the shared information $\{c_i, e_i, g_i, j_i, h(.)\}$, password PW_i and identity ID_i. This scenario still can happen in the real life. Therefore, authentication scheme should take the advantage of biometric factor to protect users.

An attacker can do the following steps to impersonate legitimate user U_i:

- Attacker U_A computes $f_i = (ID_i||PW_i) \oplus g_i$, $K_i = (ID_i||PW_i) \oplus j_i$. U_A generates a random number R_c and computes the following equations: $r_i = h(PW_i \oplus K_i) \oplus f_i$, $M_1 = c_i \oplus f_i$, $M_2 = e_i \oplus r_i$, $M_3 = M_1 \oplus R_c$, $M_4 = h(M_1||R_c) \oplus ID_i$, $M_5 = h(M_2||R_c)$. U_A sends the login request $\{M_3, M_4, M_5\}$ to S_i.
- On receiving login request $\{M_3, M_4, M_5\}$ from U_A, the server S_i firstly computes $M_6 = h(x_s||y_s)$, $M_7 = M_3 \oplus M_6$, $M_8 = h(ID_i||x_s)$, $ID_i = M_4 \oplus (M_6||M_7)$.
- S_i checks the format of ID_i. Obviously, ID_i is valid, S_i then checks if $M_5 = h(M_8||M_7)$. Of course, both are equal, S_i generates a random number R_s and computes the following equations: $M_9 = M_8 \oplus R_s$, $M_{10} = h(M_8||R_s)$. Then, S_i sends the reply message $\{M_9, M_{10}\}$ for its authentication to U_A.
- Receiving $\{M_9, M_{10}\}$ from S_i, the attacker U_A computes $M_{11} = M_9 \oplus M_2$ and checks if $M_{10} = h(M_2||M_{11})$ or not. If both are equal, U_A computes $M_{12} = h(M_2R_c||M_{11})$ and sends the reply message $\{M_{12}\}$ to S_i.
- Receiving $\{M_{12}\}$ from U_A, the server checks if $M_{12} = h(M_8M_7||R_s)$. Obviously, both are equal, S_i accepts the login request $\{M_3, M_4, M_5\}$ of U_A with U_i's identity.

Attacker U_A successfully impersonates the user U_i without U_i's biometric.

2.3 Authentication with Biometric Features

Using biometric data, a source of high-entropy information, for authentication and identity management has the following advantages: (i) not to be lost or forgotten; (ii) difficult to copy or share; (iii) hard to forge; and (iv) not to be guessed easily [7].

Together with authentication methods based on traditional biometric data, such as fingerprint, iris, voice, etc., there is a new trend to exploit body movement patterns of a user, a.k.a gait features, for identity recognition. Pan et al. use k-nearest neighbors method for gait recognition with data captured from an accelerometer [11]. Nickel and Busch propose to use Hidden Markov Model to authenticate users when they walk [14].

Among existing methods for gait recognition, Support Vector Machine is one common approach to classify users from their gait features [12, 13, 15]. Therefore, in this paper, we also follow this common trend to devise own method based on SVM for user identification based on gait feature. However, we do not use a single SVM classifier as in existing methods [12, 13, 15] but take advantages of multiple weak SVM classifiers to boost the overall accuracy.

3 Proposed Architecture and Methods for Smart Kiosk Using Gait-Based Authentication

3.1 Proposed Architecture of Smart Kiosk Using Gait-Based Authentication

Figure 1 illustrates the idea of continuous implicit authentication with gait data collected from wearable or mobile devices, such as smart watches, activity trackers, or smart phones. Gait-based user authentication has two main properties. First, it is a continuous authentication process, not a one-time operation. Therefore, it is more secure than one-time authentication schemes, such as methods with PIN or password, because the system can continuously monitor a user to ensure that the user is still a legal one. When an abnormal phenonmenon occurs, such as when a user is knocked out or falls, the current session is terminated and the authentication is restarted. Second, gait-based authentication process is performed implicitly. A user does not need to pay attention to this background process. When the user needs to prove his or her identity to a system, the current identity is available for use.

Fig. 1. Continuous implicit authentication with gait data using wearable device/mobile device

Figure 2 illustrates a typical scenario of usage at a smart kiosk using gait-based authentication. When a user arrives at a free kiosk, his or her wearable/mobile device establishes a secure communication channel with the kiosk to perform the

(a) Secure authentication (b) Using online services

Fig. 2. Secure authentication (a) and using online services (b) at Smart Kiosk with wearable device/mobile device

authentication process to the centralized Cloud Service of Smart Kiosk system using the current active user ID recognized from the device. Depending on the particular implementation, a user may be required to tap his/her device to the NFC module of a kiosk to activate the authentication process, or the process is automatically performed when the user is in the proximity of the kiosk using Bluetooth Low Energy.

Figure 3 demonstrates the architecture of the Smart Kiosk system to use biometric gait data as means of single-sign-on. The current active user ID recognized in a wearable/mobile device is transmitted via secure channel to the kiosk. Upon receiving a service request with a user ID from a kiosk, Smart Kiosk service translates the user ID into a collection of digital identities of that user, such as his or her username and password to login to the requested online service. Smart Kiosk service plays the role of an identity provider to supply appropriate digital identities to different services, relying parties. In Smart Kiosk service, we propose a mechanism to manage different online service wrappers as plugins so that new service can be added into Smart Kiosk service in the future.

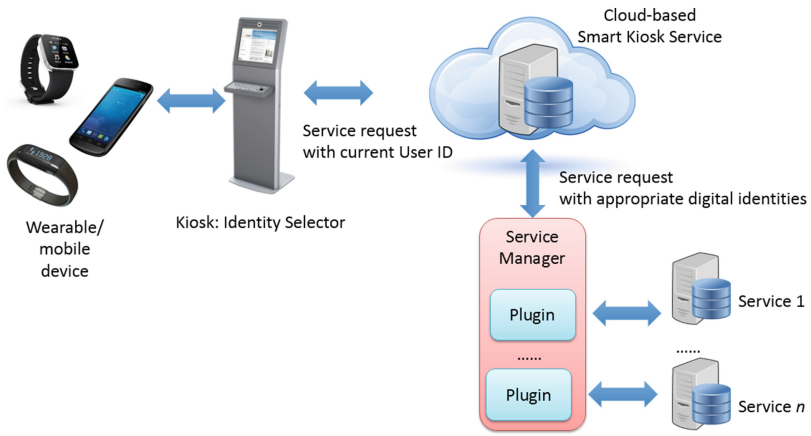

Fig. 3. Overview of the architecture to map a current user ID into appropriate digital identities for different online services

3.2 Proposed Scheme and Gait-Based Method

Our scheme includes four phases: registration, login, and mutual authentication and password-change phases. The phases are describe in detail as follow.

Registration Phase: When U_i registers with R, U_i chooses ID_i, PW_i, random nonce $K_i, K_i^{'}$ and input biometric template B_i. Then, U_i sends $\{ID_i, PW_i \oplus B_i \oplus K_i\}$ to R via secure channel.

- Step 1: When receiving registration message from U_i, R generates random value n to make different secret key at different time.
- Step 2: R computes

$$C_i = h(x_s||y_s||h(n)) \oplus h(ID_i||(PW_i \oplus B_i \oplus K_i))$$
$$e_i = h(x_s||y_s||ID_i||h(n)) \oplus h((PW_i \oplus B_i \oplus K_i)||ID_i)$$
$$f_i = h(h(x_s||y_s||h(n))||h(x_s||y_s||ID_i||h(n)))$$

Then, R sends $\{C_i, e_i, f_i, n, h(.)\}$ to U_i via secure channel

- Step 3: The user's device computes:$g_i = (ID_i||PW_i||B_i) \oplus n$,$j_i = (ID_i||PW_i) \oplus K_i$

The user hide his/her ID_i and PW_i by computes: $hID_i = ID_i \oplus h(B_i||K_i^{'})$, $hPW_i = PW_i \oplus h(K_i^{'}||B_i)$.
The user stores $\{C_i, e_i, f_i, g_i, j_i, hID_i, hPW_i, K_i^{'}, h(.)\}$ in the device.

Login Phase: To perform login phase, user's device compute the biometric B_i of U_i and flow the following steps:

- Step 1: Retrieves ID_i and PW_i by compute: $ID_i^* = hID_i \oplus h(B_i||K_i^{'})$, $PW_i^* = hPW_i \oplus h(K_i^{'}||B_i)$, $K_i^* = (ID_i^*||PW_i^*) \oplus j_i$, $n = g_i \oplus (ID_i^*||PW_i^*||B_i)$.
- Step 2: User's device compute: $M_1 = C_i \oplus h(ID_i^*||(PW_i^* \oplus B_i \oplus K_i^*))$, $M_2 = e_i \oplus h(\left(PW_i^* \oplus B_i \oplus K_i^*\right)||ID_i^*)$, and check if $f_i = h(M_1||M_2)$. If this information matches, user passes the biometrics verification; otherwise user's device terminates the session.
- Step 3: User's device generate random value R_c and compute the following equation:
  $M_3 = M_1 \oplus R_C$, $M_4 = h(R_C) \oplus ID_i$, $M_5 = h(M_2||R_c)$, $n = (ID_i||PW_i||B_i) \oplus g_i$
- Step 4: User's device sends the login request $\{h(n), M_3, M_4, M_5\}$ to S_i

Authentication with Session Key Agreement Phase: When receiving the login message, server S_i and the user's device perform the following steps to mutual authenticate:

- Step 1: S_i computes the following values:$M_6 = h(x_s||y_s||h(n))$, $M_7 = M_3 \oplus M_6$, $ID_i = M_4 \oplus h(M_7)$
- Step 2: S_i checks the format of ID_i. If ID_i is valid, S_i computes $M_8 = h(x_s||y_s||ID_i||h(n))$, and then check if $M_5 = h(M_8||M_7)$. If both equal, S_i generates a random number R_s and computes: $M_9 = M_8 \oplus R_s$, $M_{10} = h(M_8||R_s||M_7)$. Then, S_i sends the reply message $\{M_9, M_{10}\}$ for its authentication to user's device
- Step 3: On receiving $\{M_9, M_{10}\}$ from S_i the user's device computes $M_{11} = M_9 \oplus M_2$. Then, it checks if $M_{10} = h(M_2||M_{11}||R_c)$ or not. If both are equal, the device computes $M_{12} = h(M_2||R_c||M_{11})$. Then, it sends the reply message $\{M_{12}\}$ for its authentication to S_i
- Step 4: On receiving $\{M_{12}\}$, server checks if $M_{12} = h(M_8||M_7||R_s)$ or not. If both are equal, S_i accepts the login request of the user U_i.
- Step 5: U_i and S_i compute session key to encrypt exchange information after mutual authenticaion. U_i computes session key $SK = h(R_c||M_1||M_2||M_{11})$, S_i computes session key $SK = h(M_7||M_6||M_8||R_s)$.

Password Change Phase: When the user wishes to change his/her old password PW_i, the user and user's device invole folloing steps:

- Step 1: user's device compute the biometric B_i of U_i and Retrieves ID_i and PW_i by compute: $ID_i = hID_i \oplus h(B_i||K_i^{'})$, $PW_i = hPW_i \oplus h(K_i^{'}||B_i)$, $K_i = (ID_i||PW_i) \oplus j_i$. Then, user's device compute: $M_1 = C_i \oplus h(ID_i||(PW_i \oplus B_i \oplus K_i))$, $M_2 = e_i \oplus h((PW_i \oplus B_i \oplus K_i)||ID_i)$, and check if $f_i = h(M_1||M_2)$. If this information matches, user passes the biometrics verification; otherwise user's device terminates the session.
- Step 2: User input new password PW_i^*
- Step 3: User's device update the following values:

$$C_i = C_i \oplus h(ID_i||(PW_i \oplus B_i \oplus K_i)) \oplus h(ID_i||(PW_i^* \oplus B_i \oplus K_i))$$
$$e_i = e_i \oplus h((PW_i \oplus B_i \oplus K_i)||ID_i) \oplus h((PW_i^* \oplus B_i \oplus K_i)||ID_i)$$
$$g_i = g_i \oplus (ID_i||PW_i||B_i) \oplus (ID_i||PW_i^*||B_i)$$
$$j_i = j_i \oplus (ID_i||PW_i) \oplus (ID_i||PW_i^*)$$
$$hPW_i = PW_i^* \oplus h(K_i^{'}||B_i)$$

3.3 Proposed Method for Gait-Based Authentication Using Ensemble Support Vector Machine

In traditional Support Vector Machine (SVM) learning models, all samples in the training set are used to build the model. In this paper, the authors propose a modified form of SVM, which can be considered as ensembling multiple SVM classifiers to boost the overall accuracy.

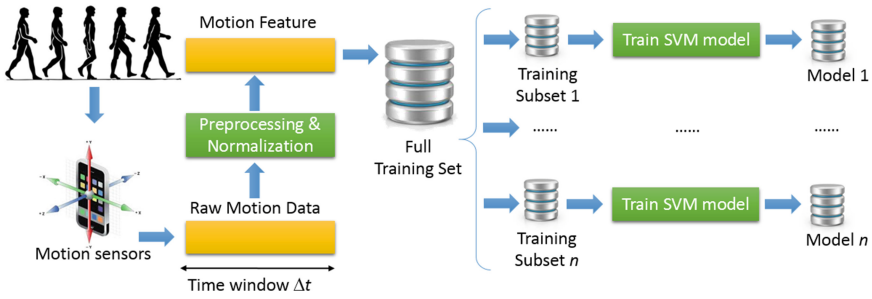

Fig. 4. Train multiple SVM classifiers with different subsets of the training set

Figure 4 demonstrates the process to train multiple SVM classifiers with different subsets of training data. Raw motion data captured from motion sensors within a pre-defined time window Δt is normalized into gait motion features. From the full

training set, we randomly create n training subsets, each of which contains P % samples from the training set. Then n lightweight SVM classifiers are trained with these training subsets. Although each of these lightweight classifiers may not be as robust as a strong classifer trained with the whole training set, ensembling all n lightweight classifiers with an appropriate voting scheme is promising to achieve higher accuracy in classification than using a single strong classifier.

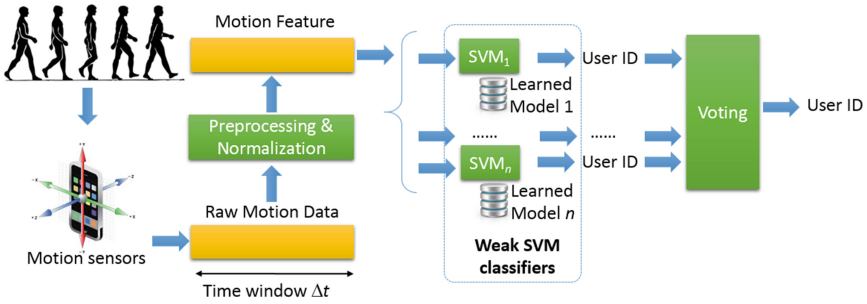

Fig. 5. User authentication with biometric gait data using multiple SVM classifiers

Figure 5 shows the main steps in our proposed SVM-based method for user identification based on his or her gait features with multiple SVM classifiers. Raw motion data is collected continuously in background mode and the process to recognize a user is activated periodically. After the preprocessing step to normalize raw motion data, motion feature is fed as an input into multiple weak SVM classifers, each of which uses a different learned model. Outputs of all these SVM classifiers are fused in the voting scheme to determine the user ID.

There are numerous measures to consolidate lightweight classifiers and voting is chosen in our proposed method. Within voting method, the predicted class of each sample is the one that has the most votes from all lightweight classifiers. If the output of classifier C_i for sample S is L_p, then class L_p has one vote from classifier C_i. Finally, if the number of votes upon class C_j exceeds the rest classes, our classification model predicts C_j as the class of sample S.

4 Security Analysis, Experiments, and Implementation

4.1 Security Analysis of Proposed Scheme and Method

In this section, we prove that our scheme is more secure than Khan et al.'s scheme by exploiting the advantage of biometric factor and can resist many kinds of attacks.

User Impersonation Attack: If an attacker wants to impersonate as a legitimate user to login the server, he/she must correctly forge the values: $h(n), M_3, M_4, M_5, M_{12}$. However, the attacker cannot do this even if he/she can extract the shared values stored in the user's device, because the attacker cannot get the value ID_i, PW_i which can only be computed based on the knowledge B_i, which is very difficult to copy or share and

extremely hard to forge. Hence, our proposed scheme can resist against the user impersonation attack.

Server Masquerading Attack: If an attacker wants to impersonate as the legitimate server S_i, he/she must forge the correct message $\{M_9, M_{10}\}$. However, since the attacker does not have the value x_s and y_s, she cannot obtain the value of M_6, M_7, M_8, and therefore cannot compute the correct M_9, M_{10}. Hence, the attacker cannot perform server masquerading attacks to fool the user.

Password Guessing Attack: Suppose the attacker can extract the secret values $\{C_i, e_i, f_i, g_i, j_i, hID_i, hPW_i, K_i^{'}, h(.)\}$ stored in the user's device, and try to derive the user's password PW_i based on some protocol transcripts. In our proposed protocol, we hide user's password by using biometric factor: $hPW_i = PW_i \oplus h(K_i^{'}||B_i)$. An attacker cannot get PW_i since the attacker does not know the user's biometrics information B_i. Moreover, our scheme does not send information contained user's password in the login and authentication scheme. Therefore, attacker cannot get any clue to guess user's password.

Replay Attack: In this kind of attack, the adversary first eavesdrops the communication flows of U_i, and later tries to imitate U_i to login S_i by replaying the eavesdropped messages. The proposed scheme using random nonce in both user and server side. These random values change randomly in each session. Therefore, the replayed message can be easily detected and dropped by S_i or U_i. Thus, the proposed scheme is capable of detecting and resisting the replay attack.

Insider Attack: In our proposed scheme, the user submits $PW_i \oplus B_i \oplus K_i$ instead of PW_i, B_i to the registration center R in the registration phase. Even though the registration server can obtain the value of K_i stored in user's device, the registration center cannot get PW_i and/or B_i, which may also be used by the user in other applications. Hence, our proposed scheme is secure against the insider attack.

Stolen Shared Information Attacks: If an attacker know the shared information $\{C_i, e_i, f_i, g_i, j_i, hID_i, hPW_i, K_i^{'}, h(.)\}$ of user U_i and wants to use this information to login to the server, he/she has to input the correct information B_i. However, B_i is very difficult to copy or share and extremely hard to forge. Therefore, the attacker cannot successfully be authenticated by the server.

Three-Factor Attack: In this kind of attack, we assume an attacker has the shared information $\{C_i, e_i, f_i, g_i, j_i, hID_i, hPW_i, K_i^{'}, h(.)\}$, password PW_i and identity ID_i of user U_i. The attacker now have to get random values n, K_i and biometric B_i to compute $h(n), M_3, M_4, M_5, M_{12}$ to authenticate with server S_i. This means the attacker have to guess three values n, K_i and biometric B_i in the same time. This can not be done in the real-time. Thus, our scheme can resist three-factor attack.

Security Comparison: In Table 2, we present the security comparison of our method with three existing schemes by Khan et al. [5], Sarvabhatla et al. [6], and Wen et al. [7]. Besides common types of attacks, our method can also resist three-factor attack which has not been considered by Sarvabhatla [6] and Wen [7].

Table 2. Comparison of ability to resist various kinds of attacks

Feature	Khan et al. [5]	Sarvabhatla et al. [6]	Wen et al. [7]	Ours
Prevent user impersonation attack	No	Yes	Yes	Yes
Prevent server masquerading attack	No	Yes	Yes	Yes
Prevent password guessing attack	No	Yes	Yes	Yes
Prevent stolen smart cards attacks	No	Yes	Yes	Yes
Mutual authentication	No	Yes	Yes	Yes
Strong replay resistance	Yes	Yes	Yes	Yes
Prevent insider attack	Yes	Yes	Yes	Yes
Three-factor attack	No	Not Consider	Not Consider	Yes

4.2 Experiment on User Recognition with Gait Data

In this experiment, we use the dataset containing 38 classes corresponding to 38 different users labeled from 1 to 38. There are 4329 samples in the training set and 4453 samples in the test set. Each feature has 288 sampling values collected from the accelerometer. The proportion ($P\%$) of training set that SVM model uses to build lightweight classifiers and the number of classifiers are two parameters in our experiment. Setting the value of P in the set {50, 60, 70, 80, 90} and the number of classifiers in the range 1 to 15, the authors probe the accuracy when using the fused model on test set. Figure 6 illustrates the result of our experiment.

As Fig. 6 shows, at the starting point (i.e. the number of classifiers is 1), using 80 % of training set results in the highest accuracy of 91.444 % while the lowest accuracy (88.996 %) is recorded when only half of the data are put into the training process. As we double the number of models, a sharp plunge is witnessed at 3 lines "80 % Training Set", "90 % Training Set", and "70 % Training Set". The other 2 lines, which is "60 % Training Set" and "50 % Training Set", experience a slight drop but the trough of accuracy (88.951 %) in our experiment is hit by the line corresponding to lower proportion of data set. When the number of models reaches 3, all lines soar

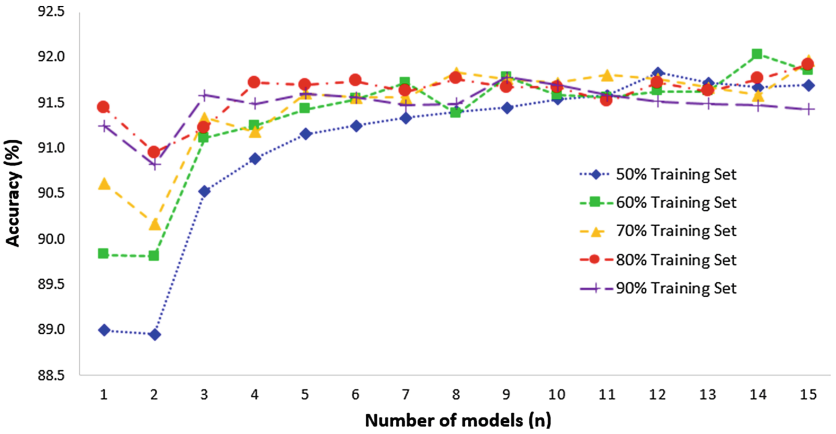

Fig. 6. Accuracy of gait-based user identification with multiple SVM classifiers

dramatically and fluctuate between 91.000 % and 92.000 % as we use more than 5 models in building the integrated classifier. By experiment, we choose the best combination of parameters as 60 % training set and 14 lightweight classifiers. In our experiment, this combination yields to 92.028 % in accuracy.

5 Conclusion

We propose Smart Kiosk system to allow users to access data and online services associated with their personal identities using implicitly continuous gait-based authentication. To realize our proposed system, we propose a user classification method based on gait data using multiple SVM classifiers and a secure authentication scheme with biometric data. In the prototype implementation of Smart Kiosk system, we use Android mobile devices for real time authentication. Currently the Smart Kiosk service can interact with Facebook, Gmail, and Flickr.

In fact, different methods to recognize users from their gait features and other schemes for user authentication can be applied into our proposed system to create different implementations. Currently, we are studying deep learning approach to learn higher-level representation of motion data captured from sensors of mobile/wearable devices for better accuracy of user identification. We also consider different strategies to devise new authentication schemes with biometric data to enhance the security for users in smart interactive environments.

Acknowledgement. This research is funded by Vietnam National University HoChiMinh City (VNU-HCM) under grant number B2015-18-01.

References

1. Lamport, L.: Password authentication with insecure communication. Commun. ACM **24** (11), 770–772 (1981)
2. Lee, C.C., Hwang, M.S., Liao, I.E.: Security enhancement on a new authentication scheme with anonymity for wireless environments. IEEE Trans. Industr. Electron. **53**(5), 1683–1686 (2006)
3. Yang, G., Wong, D.S., Wang, H., Deng, X.: Two-factor mutual authentication based on smart cards and passwords. J. Comput. Syst. Sci. **74**(7), 1160–1172 (2008)
4. An, Y.: Security analysis and enhancements of an effective biometric-based remote user authentication scheme using smart cards. J. Biomed. Biotechnol. **2012**(519723), 6 (2012)
5. Khan, M.K., Kumari, S.: (An improved biometrics-based remote user authentication scheme with user anonymity. J. Biomed. Biotechnol. **2013**(491289), 9 (2013)
6. Sarvabhatla, M., Giri, M., Vorugunti, C.S.: A secure biometrics-based remote user authentication scheme for secure data exchange. Embed. Syst. **2014**, 110–115 (2014)
7. Wen, F., Susilo, W., Yang, G.: Analysis and improvement on a biometric-based remote user authentication scheme using smart cards. J. Wireless Pers. Commun. **80**(4), 1747–1760 (2014)
8. Fan, C.I., Lin, Y.H.: Provably secure remote truly three-factor authentication scheme with privacy protection on biometrics. IEEE Trans. Inf. Forensics Secur. **4**(4), 933–945 (2009)

9. Thinh, T-T., Tran, M-T., Duong, A-D.: Robust mobile device integration of a fingerprint biometric remote authentication scheme. In: 26th IEEE International Conference on Advanced Information Networking and Applications (AINA 2012), pp. 678–685 (2012)
10. Thinh, T-T., Tran, M-T., Duong, A-D.: Robust secure dynamic ID based remote user authentication scheme for multi-server environment. In: 13th International Conference on Computational Science and Its Applications (ICCSA 2013). LNCS, vol. 7975, pp. 502–515 (2013)
11. Pan, G., Zhang, Y., Wu, Z.: Accelerometer-based gait recognition via voting by signature points. IET Electron. Lett. **45**(22), 1116–1118 (2009)
12. Frank, F., Mannor, S., Precup, D.: Activity and gait recognition with time-delay embeddings. In: The 24th AAAI Conference on Artificial Intelligence 2010, pp. 1581–1586 (2010)
13. Dandachi, G., Hassan, B.E., Hussein, A.E.: A novel identification/verification model using smartphone's sensors and user behavior. In: 2nd International Conference on Advances in Biomedical Engineering (ICABME 2013), pp. 235–238 (2013)
14. Nickel, C., Busch, C.: Classifying accelerometer data via hidden Markov models to authenticate people by the way they walk. IEEE Aerosp. Electron. Syst. Mag. **28**(10), 29–35 (2013)
15. Hoang, T., Choi, D., Vo, V., Nguyen, A., Nguyen, T.: A lightweight gait authentication on mobile phone regardless of installation error. In: The 28th IFIP TC 11 International Conference (SEC 2013), pp. 83–101 (2013)