Using Feature Fusion Strategies in Continuous Authentication on Smartphones

Yantao Li
College of Computer Science
Chongqing University
Chongqing 400044, China
Email: yantaoli@cqu.edu.cn

Bin Zou
College of Computer and Information Sciences
Southwest University
Chongqing 400715, China

Shaojiang Deng
College of Computer Science
Chongqing University
Chongqing 400044, China

Gang Zhou
Department of Computer Science
William & Mary
Williamsburg, VA 23185, USA

***Abstract*—With the increasing prevalence of mobile devices, people prefer to use smartphones to make payments, take photos, and collect personal vital information. Due to the high possibility of smartphone illegal access, the security and privacy of the devices become more important and critical. In this paper, we present *FusionAuth*, a sensor-based continuous authentication system leveraging the accelerometer, gyroscope, and magnetometer on smartphones to capture users' behavioral patterns. In order to improve the authentication performance and enhance system reliability, we are among the first to utilize two feature fusion strategies of serial feature fusion and parallel feature fusion to combine the designed features from the three sensors in the feature extraction module. Based on the trained one-class support vector domain description classifier, we evaluate the authentication performance of *FusionAuth* in terms of impact of window size and user size, and accuracy on different users. The experimental results demonstrate that *FusionAuth* reaches 1.47% mean balanced error rate (BER) with the serial fusion and achieves 1.79% mean BER with the parallel fusion.**

1. Introduction

With the increasing advancements in wireless communication technologies, mobile devices have been extensively developed in hardware and software in recent years. Tens of thousands of mobile apps have been significantly researched and created for these devices. Smart devices become more popular and pervasive, and play an important role in our daily lives. For example, according to "Number of mobile phone users worldwide from 2015 to 2020 (in billions)," there will be approximately 4.78 billion mobile phone users worldwide by 2020 [1]. According to "Number of monthly active WhatsApp users as of 2013-2017 (in millions)," there were around 1,500 million users using WhatsApp monthly on smartphones for communication in December 2017 [2]. People prefer to use smartphones to make payments, take photos, and collect personal vital information. Due to the popularity and importance of smartphones, their security and privacy become more critical to users.

To protect the security and privacy of smartphones, one-time user authentication and continuous user authentication have been investigated, successively, by researchers. One-time user authentication has been a preliminary and popular authentication mechanism that identifies users at the time of initial login, such as passcodes, PINs, graphical patterns (e.g. Gestures), fingerprints (e.g. Touch ID), and face patterns (e.g. Face ID). These approaches, however, provide limited security because they are susceptible to guessing [3], video capture [4] and spoofing [5], and they work only at the time of initial login. Subsequently, continuous authentication becomes a promising and critical authentication mechanism that frequently identifies users via their biometrics, which alleviates the above security issues. Biometrics-based approaches can be widely categorized into physiological biometrics-based and behavioral biometrics-based approaches. Physiological biometrics-based approaches rely on personal physical attributes, such as fingerprints [6] and face patterns [7], which require user direct participation. Behavioral biometrics-based approaches depend on users' behavioral patterns, such as touching [8] and gait [9]. These approaches exploit smartphone sensors to capture unique characteristics of users' movement, but ignore how to improve the representation and correlation of features.

Biometric systems that rely on a single biometric modality suffer from significant limitations due to biometric traits, noise, and poor data quality. Multibiometric systems utilize fusion to combine multiple biometric sources to improve authentication accuracy [10], [11]. Feature fusion combines features from dissimilar sensors and generates a combined feature vector. However, it is mainly used in physiological biometrics-based identification, not the behavioral biometrics-based identification.

In this paper, we present a sensor-based continuous authentication system with feature fusion, *FusionAuth*, leveraging the accelerometer, gyroscope, and magnetometer on smartphones to capture users' behavioral patterns. *FusionAuth* is composed of data collection, feature extraction, classifier, and authentication. *FusionAuth* operates in two phases: 1) the enrollment phase for learning a profile of a legitimate user, and 2) the continuous authentication phase for classifying users. Specifically, the data collection module captures users' every subtle movement during their operations on smartphones leveraging the accelerometer, gyroscope, and magnetometer. The feature extraction module

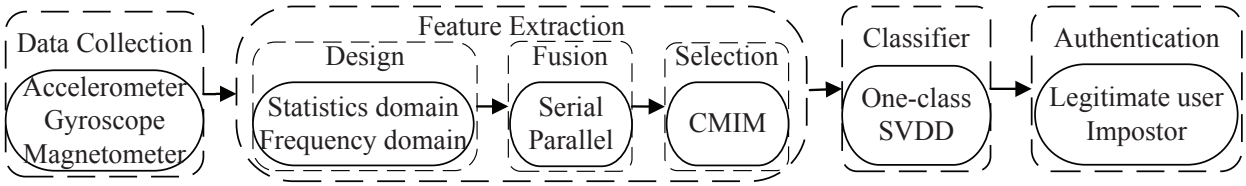

Figure 1. Architecture of *FusionAuth*

designs statistics features and frequency features that indicate the operation motions, then combines them by using the serial fusion or parallel fusion, and then selects top 5 features with the maximum mutual information by using the conditional mutual information maximization. We are among the first to exploit the two feature fusion strategies of the serial feature fusion and parallel feature fusion to combine the designed features from the three sensors for the authentication performance improvement in the feature extraction module. With the extracted features, *FusionAuth* utilizes the one-class support vector domain description to train the classifier in the enrollment phase. With the trained classifier and the testing fused feature vectors, *FusionAuth* classifies the current user as a legitimate user or an impostor in the continuous authentication phase. We evaluate the performance of *FusionAuth* in terms of the impact of time window size and user size, and accuracy on different users. The experimental results indicate that *FusionAuth* reaches 1.47% mean BER with the serial fusion and achieves 1.79% mean BER with the parallel fusion. Comparing with the existing solutions, we utilize serial feature fusion and parallel feature fusion strategies in the behavioral biometrics-based authentication.

The contributions of this work can be summarized as follows:

- We present *FusionAuth*, a smartphone user continuous authentication system that leverages existing sensors of the accelerometer, gyroscope, and magnetometer on smartphones to capture users' behavioral patterns. *FusionAuth* consists of four modules: data collection, feature extraction, classifier, and authentication.
- We are among the first to provide two feature fusion strategies - serial feature fusion and parallel feature fusion to combine the designed features from the three sensors, which can improve the authentication performance and enhance system reliability.
- We evaluate the performance of *FusionAuth* in terms of the impact of time window size and user size, and accuracy on different users, and the experimental results demonstrate that *FusionAuth* achieves 1.47% mean BER with the serial fusion and reaches 1.79% mean BER with the parallel fusion.

The rest of this paper is organized as follows. We describe the architecture of *FusionAuth* in Sec. 2, and evaluate the authentication performance in Sec. 3. Sec. 4 concludes this work.

2. System Design

In this section, we present the architecture of the continuous authentication system using feature fusion, *FusionAuth*, as illustrated in Fig. 1. As illustrated in Fig. 1, *FusionAuth* consists of four modules: 1) data collection, 2) feature extraction, 3) classifier, and 4) authentication. The operation of *FusionAuth* includes two phases for learning and classifying users' behavioral patterns: 1) the enrollment phase and 2) the continuous authentication phase. *FusionAuth* learns a profile of a legitimate user in the enrollment phase and then authenticates users in the continuous authentication phase. In particular, we provides two feature fusion strategies: serial feature fusion and parallel feature fusion in the feature extraction module to improve the authentication accuracy and enhance system reliability.

2.1. Data Collection

To collect all users' data for *FusionAuth*, we select the accelerometer, gyroscope, and magnetometer equipped on smartphones. This is because: 1) the accelerometer can record users' larger motion patterns; 2) the gyroscope can capture users' fine-grained motions; and 3) the magnetometer can measure users' ambient geomagnetic field. These three sensors do not require root permissions when they are requested by applications on smartphones, which makes them suitable for background monitoring service. In *FusionAuth*, the data collection module captures every subtle movement during the user's operation on the smartphone, and records the instantaneous readings in x, y, and z axes of the three sensors, respectively, when the screen is on. The collected data are then used for feature extraction.

2.2. Feature Extraction

The feature extraction module consists of the feature design, feature fusion, and feature selection. We first design statistics features and frequency features that capture the operation motions, then combine these features using serial fusion or parallel fusion, and then select the combined features with maximum mutual information by using the conditional mutual information maximization.

2.2.1. Feature Design. In the feature design module, with the collected sensor data, we segment them by a time period or time window. In a time window, we extract statistics

and frequency features from each axis of the accelerometer, gyroscope, and magnetometer, respectively.

Statistics features characterize the motion patterns with meaningful statistics on smartphones. We design 11 statistics features for each axis of each sensor in a time window, including the mean, median, maximum, minimum, standard deviation, range, 25%, 50%, and 75% quartiles, kurtosis, and skewness. The kurtosis feature indicates the width of peak of one-axis reading while the skewness feature represents the orientation of peak of one-axis reading. In particular, z-axis accelerometer data represent the resistance to the force exerted by user touching on smartphone screen. The range of a y-axis gyroscope data indicates the angle of smartphone rotation around the y-axis, which can discriminate between users with different rotation angles.

Frequency features capture the frequency domain information of the motion patterns, which is generated by applying the Fast Fourier Transform on sensor data. We design 5 frequency features involving the energy, entropy, HP1, FHP2, and HP2. In particular, HP1 indicates the amplitude of the first highest peak in one-axis reading in a time window. FHP2 represents the frequency of the second highest peak and HP2 denotes the amplitude of the second highest peak.

We design 16 features for each axis of each sensor, and then we have 144 features (3 axes $\times$ 3 sensors $\times$ 16 features) in total.

2.2.2. Feature Fusion. Feature fusion merges multiple features from the same or different input data and the utilization of multiple sensor features can improve the authentication accuracy and enhance system reliability. We present two feature fusion strategies: serial feature fusion and parallel feature fusion [12]. Suppose A, G, and M are three feature spaces on feature sample space Ω, indicating features of the accelerometer, gyroscope and magnetometer. For an arbitrary sample $\xi \in \Omega$, the corresponding three feature vectors are $\alpha \in A$, $\gamma \in G$, and $\mu \in M$.

The serial feature fusion combines the three feature vectors α, γ, and μ into a 144-dimensional feature ξ_s defined by $\delta_s = [\alpha, \gamma, \mu]^T$, where feature vectors α, γ and μ are 48-dimensional. All serial combined feature vectors of feature samples form a 144-dimensional serial combined feature space.

The parallel feature fusion combines α, γ, and μ into a 48-dimensional feature ξ_p defined by a complex vector $\delta_p = \alpha + i\gamma + i\mu$ (i is an imaginary unit). Note that since the dimensions of the feature vectors α, γ and μ are the same, the parallel combined feature is 48-dimensional.

2.2.3. Feature Selection. To select features with the maximum mutual information for each user from the combined serial features or combined parallel features, we conduct feature selection by using the conditional mutual information maximization (CMIM) [13]. Based on the computed mutual information between feature sets, the CMIM selects features with maximum mutual information one by one to generate an optimal feature subset. Based on the collected dataset (50 users with a sampling rate of 100 Hz, details in Sec. 3.1.1), we record the 5 most selected features for each user using the CMIM. Then, we count the number for each feature selected by all 50 users and the top 5 selected features are: 75% quartile of z and y axes of the accelerometer, 25% quartile of x axis and minimum of y axis of the magnetometer, and 75% quartile of x axis of the accelerometer.

We select top 5 features with the maximum mutual information by the CMIM for each user from the 144 designed features as the extracted features. Note that the selected top features for different users may vary.

2.3. Classifier

After features are extracted, they are passed to a classifier for training and testing, respectively. We implement the one-class support vector domain description (SVDD) classifier. The goal of SVDD is to find a sphere with minimum volume, containing all (or most of) the data objects [14]. These data objects can be regarded as one class.

In the enrollment phase, the one-class SVDD classifier is trained by the extracted features of the owner's data with a radial basis function (RBF) kernel. To train the classifier, we randomly select 50% positive samples (legitimate data) as the training dataset. The remaining 50% with all the negative samples (impostor's data) are used as the testing dataset for classifier testing. In the training phase, two parameters C and σ need to be optimized, where C is the volume factor, controlling the number of samples that fall into the decision boundary, and σ is used to calculate the primal problem, controlling the width of the RBF kernel. We utilize a grid search over the parameter space to perform the parameter optimization, and use the cross-validation to avoid over fitting. In the continuous authentication phase, the trained SVDD classifier finds a bounding sphere with minimum radius, containing most of the positive samples.

2.4. Authentication

Based on the serial or parallel fused features and the trained SVDD classifier, Authentication classifies the current user as a legitimate user or an impostor. If the current user is classified as an impostor, *FusionAuth* will require initial login inputs; otherwise, it will continuously authenticate the user.

3. Performance Evaluation

In this section, to evaluate the performance of *FusionAuth*, we first elaborate the experiment setup including dataset, classifier training and metrics, and then provide the experimental results in terms of the impact of time window and user number, and accuracy.

3.1. Experiment Setup

In this section, to set up the experiments, we first describe how to collect the data from the three sensors. Then,

we discuss how to select appropriate parameters for the one-class SVDD classifier and how to train the classifier. Finally, we introduce three representative metrics for the evaluation of the authentication accuracy of *FusionAuth*.

3.1.1. Dataset. To collect sensor data, we recruited 100 users (53 male and 47 female) interacting with ten Samsung Galaxy S4 smartphones [15]. When they started operating on smartphones, they were randomly assigned one of the three scenarios: document reading, text production, and navigation on a map. Each user was designed to perform about 24 sessions (8 reading sessions, 8 writing sessions, and 8 map navigation sessions) and each session lasted about 5 to 15 minutes. The collected sensor data were stored in .CSV files on smartphones.

To evaluate *FusionAuth*, we select sensor data of the accelerometer, gyroscope, and magnetometer from 50 users including 25 male and 25 female with a sampling rate of 100 Hz.

3.1.2. Classifier training. With the extracted features for 50 users, we design the training procedure for the one-class SVDD with a radial basis function as the kernel function:

Step 1 (User selection): Randomly select one user from the 50 users as a legitimate user and the rest 49 users as impostors. The legitimate user's data are labeled as positive samples and impostors' data as negative samples.

Step 2 (Training set and testing set): Randomly select 50% of the positive samples as the training set and the rest 50% with all the negative samples are used as testing set.

Step 3 (Parameter optimization): Utilize grid search over parameter space to find optimal values for parameters C and σ.

We obtain one classification model for each user each procedure (from Step 1 to Step 3), and then we can obtain 50 classification models for 50 users. Since the training set are randomly selected, we repeat the procedure 10 times for each user.

3.1.3. Metrics. To evaluate the authentication accuracy of *FusionAuth*, we select three representative metrics in our evaluation: false acceptance rate (FAR), false rejection rate (FRR), and balanced error rate (BER) [14]. The FAR is the probability that an impostor is falsely classified as a legitimate user, defined as: $FAR = \frac{\#\ of\ false\ acceptances\ (FP)}{\#\ of\ attempts\ by\ impostors\ (FP+TN)}$. The FRR is the probability that a legitimate user is incorrectly identified as an impostor, defined as: $FRR = \frac{\#\ of\ false\ rejections\ (FN)}{\#\ of\ attempts\ by\ legitimate\ users\ (FN+TP)}$. The BER is an equally weighted combination of the FAR and the FRR, defined as: $BER = \frac{FAR+FRR}{2}$, and a lower BER indicates higher authentication accuracy.

3.2. Experimental Results

In this section, based on the experiment setup, we evaluate the performance of *FusionAuth*. Specifically, we first explore the impact of time window size and impact of user size on the authentication accuracy and then evaluate the system authentication accuracy on different users by using the serial fused features and parallel fused features.

3.2.1. Impact of time window. In the feature extraction module, we set a time window for the collected sensor data and extract features from each time window. The length of the time window determines the period and data amount for the user authentication.

We explore the impact of different time window sizes from 1s to 15s with a 1s interval. Based on the experiment, we plot the BERs against different time window sizes for *FusionAuth* using serial fusion and parallel fusion, respectively, in Fig. 2. As shown in Fig. 2, both the BERs decrease with the increase of the window size. In particular, both BERs decrease rapidly until 9s and then keep steady. Considering the authentication frequency and the accuracy, we set the time window size as 9s for *FusionAuth* in the experiments.

3.2.2. Impact of user size. To show the advantage of our fusion strategies, we compare the accuracy of *FusionAuth* using serial fusion and parallel fusion strategies with that using non fusion strategy. From the feature extraction module, supposing the designed features are $F_\alpha = \{F_{\alpha 1}, F_{\alpha 2}, ..., F_{\alpha 48}\}$ for the accelerometer, $F_\gamma = \{F_{\gamma 1}, F_{\gamma 2}, ..., F_{\gamma 48}\}$ for the gyroscope, and $F_\mu = \{F_{\mu 1}, F_{\mu 2}, ..., F_{\mu 48}\}$ for the magnetometer, the non fusion feature is obtained by $F_{Non} = (\sqrt{F_{\alpha 1}^2 + F_{\gamma 1}^2 + F_{\mu 1}^2}, \sqrt{F_{\alpha 2}^2 + F_{\gamma 2}^2 + F_{\mu 2}^2}, ..., \sqrt{F_{\alpha 48}^2 + F_{\gamma 48}^2 + F_{\mu 48}^2})$. In the system architecture, we implement non fusion by replacing feature fusion with F_{Non}.

To investigate the impact of user size on the authentication accuracy, we train the classifier with 10 different user sizes, ranging from 5 to 50 with stride 5. We plot the BERs against 10 different user sizes for serial fusion, parallel fusion, and non fusion strategies, respectively, in Fig. 3. As illustrated in Fig. 3, with the increase of the user number, the BER gradually decreases and becomes steady at around 1.56%. In addition, the BERs of *FusionAuth* using fusion strategies are lower than that without fusion. The serial fusion strategy achieves the lowest BER at 1.47% with 45 users while the parallel fusion strategy reaches the lowest BER at 1.49% with 25 users.

3.2.3. Accuracy on different users. To evaluate the adaptability of *FusionAuth* to different users, we conduct experiments to calculate the user authentication accuracy for each of the 50 users, as depicted in Fig. 4. As shown in Fig. 4, the mean BERs of the two fusion strategies for each user are lower than that of non fusion strategy. In addition, using the two strategies, the mean BERs are around 1%-2% for most of the users. We calculate the mean, minimum and maximum of BER for the three strategies for all the 50 users. The results indicate the serial fusion and parallel fusion achieve 1.47% and 1.79% mean BER, respectively, while non fusion reaches 5.31% mean BER. For the two fusion

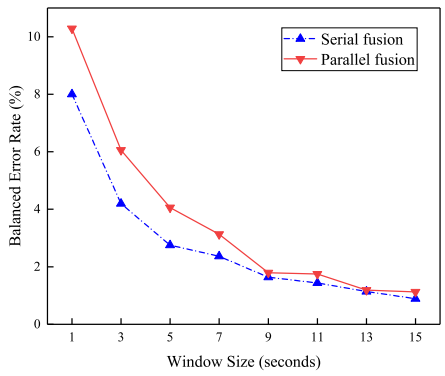

Figure 2. Impact of time window

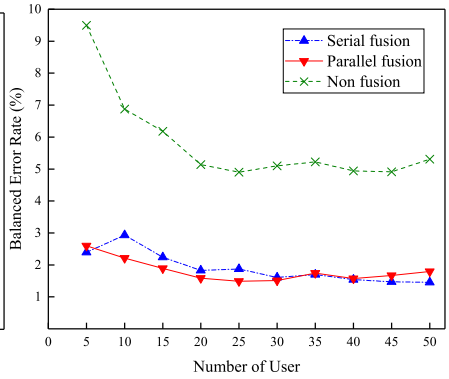

Figure 3. Impact of user number

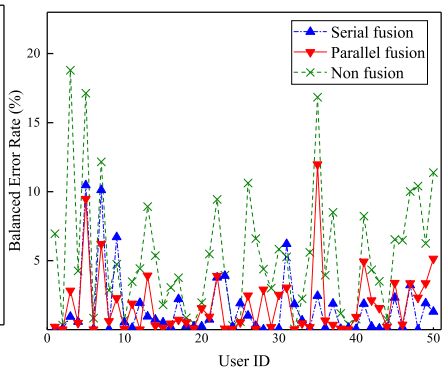

Figure 4. Accuracy on different users

strategies, they have almost the same statistic performance. Moreover, the serial fusion shows the lowest maximum BER (10.46%) while the parallel fusion has the lowest minimum BER (0.01%).

In order to compare the performance of the serial fusion and parallel fusion, we compute the FAR and FRR for *FusionAuth*. According to the results, the FRR of the parallel fusion (0.74%) is better than that of the serial fusion (1.05%) while the FAR of the serial fusion (1.89%) is better than that of the parallel fusion (2.85%). That is, *FusionAuth* using the parallel fusion rarely rejects legitimate users, and *FusionAuth* using the serial fusion rarely accepts impostors.

4. Conclusion

To address the security and privacy issues on mobile devices, we present a sensor-based continuous authentication system, *FusionAuth*, leveraging the accelerometer, gyroscope, and magnetometer on smartphones to capture users' behavioral patterns. *FusionAuth* consists of four modules: data collection, feature extraction, classifier, and authentication. We are among the first to utilize two feature fusion strategies of serial feature fusion and parallel feature fusion to combine the designed features from the three sensors. We evaluate the authentication performance of *FusionAuth* and the experimental results demonstrate that both the serial fusion and the parallel fusion greatly improve the authentication accuracy of the system.

Acknowledgments

We thank the subjects for collecting the experimental data and appreciate the anonymous reviewers for their valuable suggestions. This work was supported by the National Natural Science Foundation of China under Grant 61672119.

References

[1] Number of mobile phone users worldwide from 2015 to 2020 (in billions). 2018. [Online]. Available: https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

[2] Number of monthly active whatsapp users worldwide from april 2013 to december 2017 (in millions). 2019. [Online]. Available: https://cdn.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

[3] PIN Analysis. 2019. [Online]. Available: http://www.datagenetics.com/blog/september32012/

[4] D. Shukla, R. Kumar, A. Serwadda and V. V. Phoha, "Beware, your hands reveal your secrets!" in *Proc. ACM SIGSAC Conf. Comput. Commun. Security*, New York, NY, USA, 2014, pp. 904-917.

[5] Fingerprints are not fit for secure device unlocking. 2019. Available: https://srlabs.de/bites/spoofing-fingerprints/

[6] N. Shabrina, T. Isshiki and H. Kunieda, "Fingerprint authentication on touch sensor using phase-only correlation method," in: *Proc. 7th Int. Conf. Inf. Commun. Tech. Embedded Syst.*, Bangkok, Thailand, 2016, pp. 15.

[7] P. Perera and V. M. Patel, "Face-Based Multiple User Active Authentication on Mobile Devices," *IEEE Trans. Inf. Forensics Security,* vol. 14, no. 5, pp. 1240-1250, 2018.

[8] B. Zou and Y. Li, "Touch-based Smartphone Authentication Using Import Vector Domain Description," in: *Proc. 29th Int. Conf. Application-specific Syst., Architectures and Processors*, Milan, Italy, 2018, pp. 85-88.

[9] Y. Ren, Y. Chen, M. C. Chuah and J. Yang, "User Verification Leveraging Gait Recognition for Smartphone Enabled Mobile Healthcare Systems," *IEEE Trans. Mobile Comput.,* vol. 14, no. 9, pp. 1961-1974, 2015.

[10] Y. Ding and A. Ross, "A comparison of imputation methods for handling missing scores in biometric fusion," *Pattern Recognit.*, vol. 45, no. 3, pp. 919-933, 2012.

[11] Y. Li, H. Hu and G. Zhou, "Using Data Augmentation in Continuous Authentication on Smartphonesn," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 628-640, 2019.

[12] J. Yang, J.-Y. Yang, D. Zhang and J.-F. Lu, "Feature fusion: parallel strategy vs. serial strategy," *Pattern Recognit.*, vol. 36, no. 6, pp. 1369-1381, 2003.

[13] F. Fleuret, "Fast Binary Feature Selection with Conditional Mutual Information," *J. Mach. Learn. Res.*, vol. 5, pp. 1531-1555, 2004.

[14] D.M.J. Tax and R.P.W. Duin, "Support vector domain description," *Pattern Recogn. Lett.*, vol. 20, no. 11-13, pp. 1191-1199, 1999.

[15] Z. Sitova, J. Sedenka, Q. Yang, G. Peng, G. Zhou, P. Gasti and K.S. Balagani, "HMOG: New Behavioral Biometric Features for Continuous Authentication of Smartphone Users," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 877-892, 2016.

Yantao Li is a Professor with the College of Computer Science, Chongqing University, Chongqing, China. He

received the Ph.D. degree from the College of Computer Science, Chongqing University, China, in December 2012. His research area includes wireless communication and networking, sensor networks and ubiquitous computing, and information security. He was a recipient of the Outstanding Ph.D. Thesis Award in Chongqing in 2014, and the Outstanding Master's Thesis Award in Chongqing in 2011. Contact him at yantaoli@cqu.edu.cn.

Bin Zou is an Engineer at CMB Network Technology, Chengdu, China. He received the M.S. and B.S. degrees from the College of Computer and Information Sciences, Southwest University, Chongqing, China, in June 2019 and June 2016, respectively. Contact him at 1184142494@qq.com.

Shaojiang Deng is a Professor with the College of Computer Science, Chongqing University, Chongqing, China. He received the Ph.D. degree from the College of Computer Science, Chongqing University, China, in June 2005. His research interests include information security, mobile computing, wireless sensor networks. Contact him at sj_deng@cqu.edu.cn.

Gang Zhou is a Professor in the Computer Science Department at William & Mary. He was Graduate Program Director from 2015 to 2017. He received his Ph.D. degree from University of Virginia in 2007. He has published more than 100 papers in prestigious conferences and journals. His Google Scholar Citations are over 8000, with h-index 33 and i10-index 73. He received an NSF CAREER Award in 2013, the Best Paper Award of IEEE ICNP 2010, and Plumeri Award for Faculty Excellence in 2015. Dr. Zhou serves on the Journal Editorial Board of ACM Transactions on Computing for Healthcare (HEALTH), ACM Transactions on Sensor Networks (TOSN), Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT), and Elsevier Smart Health. He also served on the Journal Editorial Board of IEEE Internet of Things and Elsevier Computer Networks. He serves as a Steering Committee member, General Chair, and TPC Chair of CHASE - ACM/IEEEs premier conference on Connected Health: Applications, Systems and Engineering Technologies. Contact him at gzhou@cs.wm.edu.