Authentication Methods for Mobile Device Users

Subjects: Computer Science, Artificial Intelligence

Contributor: Zhengqiu Weng , Shuying Wu , Qiang Wang , Tiantian Zhu

With the advent of smart mobile devices, end users get used to transmitting and storing their individual privacy in them, which, however, has aroused prominent security concerns inevitably. Numerous researchers have primarily proposed to utilize motion sensors to explore implicit authentication techniques.

mobile user authentication | deep learning | large-scale data analysis | implicit authentication

1. Introduction

With the advancement of mobile communication technology and hardware updates, mobile intelligent terminal devices have become increasing popular and are widely used in people's daily lives. The mobile application market has an anticipated annual consumer spending of USD 233 billion on the Apple App Store and Google Play store in 2022–2026 [1]. According to Grand View Research, the global mobile application market is expected to grow at a compound annual growth rate (CAGR) of 13.4% from 2022 to 2030 [2]. As more and more users transmit and even store their private data in mobile devices, it becomes very important to avoid information leakage in the network attack and defense. Especially in the instance where users are part of organizations such as enterprises, governments, and national infrastructure, the information leakage caused by advanced persistent threat attacks, conducted mainly by accessing the mobile devices to collect valuable confidential information, would be a catastrophe. Therefore, in order to safeguard their privacy and security, it is urgent to design suitable and robust user authentication models based on both the application scenarios and the features of mobile devices.

The current authentication methods for mobile users can be broadly categorized into two types: knowledge-based and biometric-based. Knowledge-based authentication methods [3] require users to explicitly input information such as passwords or patterns. Although these methods are widely used due to their low cost, they have to face challenges from the perspective of usability and security [4][5]. For example, (1) they are prone to various attacks such as brute force, shoulder surfing, smudge, inference, and social engineering attacks, and (2) inputting the same password repeatedly in small dialog boxes would have impact on the user physical experience. In contrast, biometric-based authentication methods [6] can mitigate the above issues to some extent. However, frequently using the facial or fingerprint recognition may also, especially in some ungoverned scenarios, bring psychological discomfort. Therefore, both usability and security should be the priority for the authentication systems. Recently, there has been extensive research on user dynamic authentication methods based on motion sensors. These methods identify users' information with machine learning or deep learning methods to discern unique behavioral patterns through their gait/gestures, because no privacy-related permissions are required in motion sensors. Then,

researchers collect a series of non-privacy motion sensor data, such as accelerometer, gravity sensor, and gyroscope sensor data (through the system-level interface any application can obtain the data). However, in real-world and complex environments, it is hard to distinguish user micro features. The major challenges are as follows:

(1) In mobile user authentication, the majority of sensory signal transformation methods rely on expert knowledge [7][8]. They lack the in-depth data mining of motion sensor signals, and they are unable to effectively learn the complex nonlinear relationships between invariant features.

(2) Label noise is widely present in the training phase, e.g., device owners lend their phones to others. Most research has paid more attention to signal denoising, but less to reducing label noise [9][10]. If a classifier is trained with incorrect labels, continuous errors can accumulate. Even if labeled samples are obtained from the target person, the classifier may still fail to authenticate the device owner.

(3) The quality of handmade features is crucial for the performance of most classifiers. However, when dealing with complex mixed motion sensor signals, relying solely on statistical features can lead to critical information loss [7][11][12][13]. Additionally, the feature extraction process is typically fixed by the determined algorithm, whereas iterative optimization can be used to update the parameters of the classification model. This can hinder the improvement of algorithms for sensor-based mobile user authentication.

2. Authentication Methods

Mobile device user authentication methods are essential for protecting user data. Currently, they can primarily be classified into three types: knowledge-based methods [5], static feature-based methods [6], and dynamic behavior-based methods [7]. Knowledge-based methods require users to explicitly enter a digital password or gesture pattern to unlock the mobile device or log into an application. These methods can only verify whether a user knows the credential but cannot determine whether the user is the device owner. Furthermore, they pose certain risks, such as poor human–computer interaction experience and privacy leakage. Previous studies have shown that they can easily be broken by brute force attacks [14], smudge attacks [15], shoulder surfing attacks [16], and sensor inference [17]. In contrast, static biometric authentication methods are based on fingerprints and faces, which can achieve relatively high recognition accuracy [18][19][20]. However, except concerns about the user experience and privacy leakage mentioned in Section 1, recent research has shown that misusing fingerprint APIs on Android can make applications vulnerable to various attacks [18], and face recognition methods based on deep learning algorithms have been proven to be circumvented by sophisticated attackers [19][20]. Dynamic behavior-based authentication methods access data from built-in sensors in mobile devices, including environmental locations, keystroke behaviors, finger movements, etc., and they work through the combination of feature engineering and model training. These methods may call privacy-related permissions to obtain user privacy data.

Static/dynamic feature authentication methods are based on credential technology and privacy risks. Given their inherent drawbacks, numerous researchers [8][11][12][13][21][22][23][24][25][26] proposed dynamic user authentication based on motion sensors, which has the following limitations: First, most user authentication based on motion

sensors requires a user to use their phone at a fixed location or perform specific actions (in a lab environment), which is unrealistic and results in a large number of noisy labels in complex environments (non-lab environments). Second, the credibility of the data collected in complex environments is often questionable, for example, unreliable labels are generated if the phone is used by others except the owner. To achieve both good user experience and high authentication accuracy simultaneously, this research proposes an effective sensor-based mobile user authentication method in complex environments.

Data denoising method for sensor-based mobile user authentication. Currently, most dynamic authentication methods utilize motion sensors [8][9][10][11][12][13][21][22][23][24][25][26]. They do not consider the impact of hardware noise. Then, it is very difficult for them to handle unlabeled data (noise data) in real environments. Finally, overfitting occurs and authentication accuracy decreases. In order to address the noise, some researchers [8] proposed noise elimination algorithms to obtain an effective dataset in the data preprocessing stage, but these algorithms cannot precisely distinguish the mislabeled and training samples. To overcome it, researchers used semi-supervised methods, combining noisy data with a set of clean labels [7]. Zhu et al. [7][8][9] observed that flat data cannot reflect the discrepancies of different user patterns in its collection. Removing it will omit analyzing its usability. Additionally, when collecting users' data, researchers find the data are often mislabeled, such as unreliable labels researchers mentioned above. This research simultaneously considers the noise and mislabeled data during the training process, fitting the training requirements to the greatest extent to provide high-quality data.

Mobile user authentication model based on motion sensors. The existing research methods using motion sensors [8][9][10][11][12][13][21][22][23][24][25][26] continuously collect sensor data and establish corresponding models to verify users' ID. Lu et al. [24] used unsupervised learning algorithms to process unlabeled data, but this method resulted in high latency. Additionally, unsupervised clustering algorithms with parameter adjustment have high overhead, and the parameter's generalization needs to be verified. Zhu et al. [7] designed a semi-supervised online learning algorithm. It has a high level of accuracy and low latency in processing unlabeled data under relatively complex environments, but the classification they used (binary class SVM) is not applicable to time series data due to ignoring the context of user behaviors. Furthermore, most existing studies [8][9][10][11][12][13][21][22][23][24][25][26] assume the input data are sufficient, which is not considered in real complex environments. In contrast, this research proposes the transformation of 1D signals into 2D images. Meanwhile considering the spatio-temporal characteristics of sensory signals, researchers extract spatio-temporal features using CNN to achieve high mobile user authentication accuracy.

References

1. Store Intelligence Data Digest Report. 2022. Available online: https://sensortower.com/resources (accessed on 6 July 2023).
2. Mobile Application Market Size, Share & Trends Report. 2030. Available online: https://www.grandviewresearch.com/industry-analysis/mobile-application-market (accessed on 6

July 2023).

3. Alhakami, H.; Alhrbi, S. Knowledge based Authentication Techniques and Challenges. Int. J. Adv. Comput. Sci. Appl. 2020, 11, 1–6.
4. Dee, T.; Richardson, I.; Tyagi, A. Continuous nonintrusive mobile device soft keyboard biometric authentication. Cryptography 2022, 6, 14.
5. Bošnjak, L.; Brumen, B. Examining security and usability aspects of knowledge-based authentication methods. In Proceedings of the 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 20–24 May 2019.
6. Ray-Dowling, A.; Hou, D.; Schuckers, S. Stationary mobile behavioral biometrics: A survey. Comput. Secur. 2023, 128, 103184.
7. Zhu, T.; Qu, Z.; Xu, H.; Zhang, J.; Shao, Z.; Chen, Y.; Yang, J. RiskCog: Unobtrusive real-time user authentication on mobile devices in the wild. IEEE Trans. Mob. Comput. 2019, 19, 466–483.
8. Ren, Y.; Chen, Y.; Chuah, M.C.; Yang, J. User verification leveraging gait recognition for smartphone enabled mobile healthcare systems. IEEE Trans. Mob. Comput. 2015, 14, 1961–1974.
9. Zhu, T.; Weng, Z.; Song, Q.; Chen, Y.; Liu, Q.; Chen, Y.; Chen, T. Espialcog: General, efficient and robust mobile user implicit authentication in noisy environment. IEEE Trans. Mob. Comput. 2020, 21, 555–572.
10. Zhu, T.; Weng, Z.; Chen, G.; Fu, L. A hybrid deep learning system for real-world mobile user authentication using motion sensors. Sensors 2020, 20, 3876.
11. Sitová, Z.; Šeděnka, J.; Yang, Q.; Peng, G.; Zhou, G.; Gasti, P.; Balagani, K.S. HMOG: New behavioral biometric features for continuous authentication of smartphone users. IEEE Trans. Info. Forensics Secur. 2015, 11, 877–892.
12. Shen, C.; Li, Y.; Chen, Y.; Guan, X.; Maxion, R.A. Performance analysis of multi-motion sensor behavior for active smartphone authentication. IEEE Trans. Info. Forensics Secur. 2017, 13, 48–62.
13. Lee, W.H.; Lee, R.B. Multi-sensor authentication to improve smartphone security. In Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP), Angers, France, 9–11 February 2015; pp. 1–11.
14. Zoebisch, F.; Vielhauer, C. A test tool to support brute-force online and offline signature forgery tests on mobile devices. In Proceedings of the 2003 International Conference on Multimedia and Expo(ICME), Baltimore, MD, USA, 6–9 July 2003; p. III-225.

15. Aviv, A.J.; Gibson, K.; Mossop, E.; Blaze, M.; Smith, J.M. Smudge attacks on smartphone touch screens. In Proceedings of the 4th USENIX Conference on Offensive Technologies, Berkeley, CA, USA, 23–25 June 2010; pp. 1–7.
16. Zakaria, N.H.; Griffiths, D.; Brostoff, S.; Yan, J. Shoulder surfing defence for recall-based graphical passwords. In Proceedings of the Seventh Symposium on Usable Privacy and Security, Washington, DC, USA, 20–22 July 2011; pp. 1–12.
17. Xu, Z.; Bai, K.; Zhu, S. Taplogger: Inferring user inputs on smartphone touchscreens using on-board motion sensors. In Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks, New York, NY, USA, 16–18 April 2012; pp. 113–124.
18. Bianchi, A.; Fratantonio, Y.; Machiry, A.; Kruegel, C.; Vigna, G.; Chung, S.P.H.; Lee, W. Broken fingers: On the usage of the fingerprint API in android. In Proceedings of the NDSS, San Diego, CA, USA, 18–21 February 2018; pp. 1–15.
19. Sharif, M.; Bhagavatula, S.; Bauer, L.; Reiter, M.K. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In Proceedings of the 2016 ACM Sigsac Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1–12.
20. Goswami, G.; Ratha, N.; Agarwal, A.; Singh, R.; Vatsa, M. Unravelling robustness of deep learning based face recognition against adversarial attacks. In Proceedings of the AAAI Conference on Artificial Intelligence, New Orleans, LA, USA, 2–7 February 2018; pp. 1–8.
21. Kwapisz, J.R.; Weiss, G.M.; Moore, S.A. Cell phone-based biometric identification. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems, Washington, DC, USA, 27–29 September 2010; pp. 1–7.
22. Ho, C.C.; Eswaran, C.; Ng, K.W.; Leow, J.Y. An unobtrusive android person verification using accelerometer based gait. In Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia, Bali, Indonesia, 28–30 November 2012; pp. 271–274.
23. Zhu, J.; Wu, P.; Wang, X.; Zhang, J. Sensec: Mobile security through passive sensing. In Proceedings of the 2013 International Conference on Computing, Networking and Communications, San Diego, CA, USA, 28–31 January 2013; pp. 1128–1133.
24. Lu, H.; Huang, J.; Saha, T.; Nachman, L. Unobtrusive gait verification for mobile phones. In Proceedings of the 2014 ACM International Symposium on Wearable Computers, Seattle, WA, USA, 13–17 September 2014; pp. 91–98.
25. Lee, W.H.; Liu, X.; Shen, Y.; Jin, H.; Lee, R.B. Secure pick up: Implicit authentication when you start using the smartphone. In Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies, Indianapolis, IN, USA, 21–23 June 2017; 2017; pp. 67–78.
26. Buriro, A.B.; Crispo, B.; Zhauniarovich, Y. Please hold on: Unobtrusive user authentication using smartphone’s built-in sensors. In Proceedings of the 2017 IEEE International Conference on

Identity, Security and Behavior Analysis, New Delhi, India, 22–24 February 2017; pp. 1–8.