International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 10, Number 2, pages 189–199, July 2020

Redefine and Organize, 4th Authentication Factor, Behavior

Rie Shigetomi YAMAGUCHI, Toshiyuki Nakata, Ryosuke Kobayashi
Social ICT Research Center,
Graduate School of Information Science and Technology,
The University of Tokyo,
7-3-1 Hongo, Bunkyo, Tokyo 113-8657, JAPAN

Received: February 10, 2020
Revised: May 4, 2020
Accepted: June 2, 2020
Communicated by Toru Nakanishi

Abstract

While the use of intelligent devices such as smartphones is spreading rapidly, for the most part, people continue to rely on old ID/password methods for authentication purposes, and the modernization of authentication technology is recognized as an ongoing challenge for society. In the face of this challenge, one form of authentication technology that has been attracting significant attention recently promotes the use of information technology (IT) to identify people based on information about their habits. In application, this technology obtains information about users from smartphones and wearable devices and thus performs authentication without requiring them to perform any verification operations. This is accomplished by redefining and organizing a fourth personal authentication factor, behavior. Herein, we discuss the recent trends of this technology as part of smartphone society, define the technical issues that must be resolved for realizing behavior authentication, and describe measures for resolving them.

Keywords: Personal Authentication, Behavior Authentication, Lifestyle Authentication

1 Introduction

The use of information technology (IT) in providing infrastructure for various facilities has recently become commonplace. As IT combines with new technologies such as artificial intelligence (AI) and the Internet of Things (IoT), a new society has emerged. These AI/IoT technological advancements have changed our lives by ushering in a range of novel technologies such as interactive robots, autonomous vehicles, and improvements to procedures for disease prediction, health management, insurance reviews, and many others. In light of these advancements, it is necessary to redesign our society based on the assumption that IT exists independently, rather than by converting traditional pen and paper approaches into IT forms. Ultimately, the most important objective is the creation of a safe and comfortable society [5].

One of the areas that require serious attention is the framework of payment systems, which, due to various technological changes, are now in the process of constant revision. As examples, barcode settlements using smartphones are now available in many countries, and Amazon has put forth a service called Amazon Go [37], in which shoppers swipe their smartphones to provide authentication when entering a store. However, the majority of all online personal authentication services still use ID/password combinations.

The problems related to ID/password authentication programs have existed for many years [1], and numerous improvements to these authentication technologies have been suggested. Furthermore, although it is easy to point out problems of these new developments, it is also clear that the root cause of those problems is being neglected.

In this paper, we will discuss why ID/password services are still in use and then discuss the requirements for new authentication measures. Additionally, in light of the growing popularity of fourth factor authentication (4FA) as a new security paradigm for smartphone society, we will redefine a fourth authentication factor, behavior, to point out the concept of time and take several factors such as location or life log data. Although numerous people have already pointed out that this factor faces problems, especially in the area of privacy protection, the factor is already in use by some services, so it will be necessary to address those problems as well.

1.1 Contents

The remainder of this paper is organized as follows. In Section 2, we discuss ID/password authentication problems. In Section 3, we describe the current state of social exchange. In section 4, we arrange the things to look out for before the discussion for new factor. In Section 5, we explain in detail how we will use "behavior" as a fourth factor. Section 6 is the discussion section. Finally, we present our conclusions.

2 ID/password problem has existed for 40 years

Problems with the ID/password model have existed for 40 years [1]. In fact, more than 20 years ago, when the Internet was still relatively new, potential solutions to ID/password-related problems had already been suggested in numerous studies [28].

However, while there have been countless proposals aimed at creating systems that can be substituted for ID/password-based authentication, such as smartcard systems, biometric sensors, and one-time password tokens, there has yet to be new technologies that could completely replace ID/password-based authentication systems.

2.1 Current survey on EC sites

Most sites rely on ID/password authentication, primarily because such systems are inexpensive and convenient. In 2016, Symantec inc., which was recently renamed NortonLifeLock Inc., sent questionnaires to 300 corporate E-Commerce (EC) website administrators site [31] in which one of the questions asked was, "What kind of user authentication is currently carried out on your company's site?" Although multiple answers were allowed, 77.3% of the administrators said their EC sites still used ID/password authentication, as shown in figure 1.

Another issue of concern is the fact that users tend to reuse the same passwords. In 2016 in a Symantec questionnaire in which responders were asked if they used different passwords for separate payment services, 62% of the 245 users that responded said they used between one and three different ID/password combinations, as shown in figure 2 [31]. Additionally, in the services provided by Yahoo! JAPAN, it was learned that approximately 15,000 password resets occur daily due to users forgetting their passwords [12].

The reality is, numerous users are unable to remember their passwords.

2.2 Other authentication methods have different problems

In order to address this problem, various authentication methods that do not rely on the user memory, such as the use of biometric sensors, have been proposed. Biometrics is an is an extremely accurate and very useful authentication method that uses the physical features of the user, so that users do not need to remember anything to perform authentication [35]. However, several problems

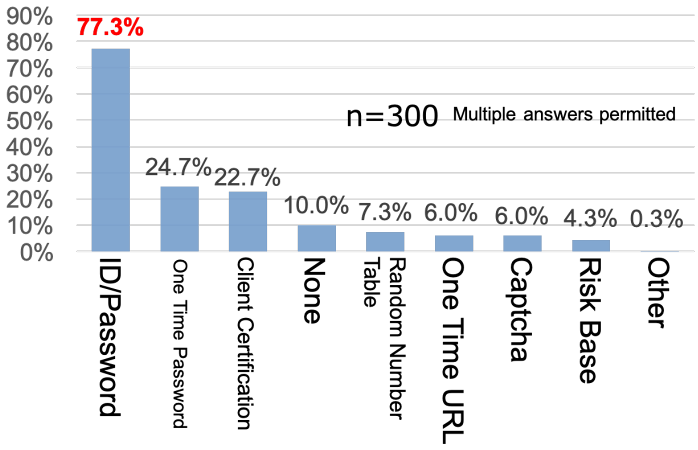

Figure 1: Q: What kind of user authentication is currently carried out on your company's site?

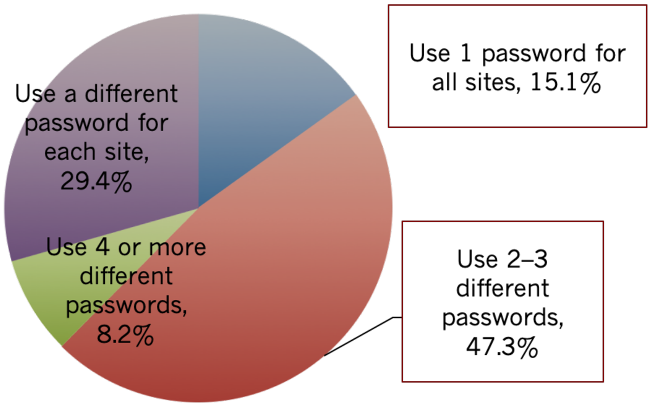

Figure 2: Q: Do you use different passwords for each payment service?

with using this factor have been pointed out. First, biometric authentication methods are currently under increasingly heavy attack [8]. Moreover, since biometric information (such as fingerprints) cannot be changed, it is impossible to prevent spoofing by updating the authentication data once such information has been leaked. This means that the only remedy is to stop using that information for the authentication system.

An alternative method is to provide users with more advanced tools, which can be hardware or software, for use as authentication factors. Such tools, which include integrated circuit (IC) cards or one-time password tokens, are very strong against several types of vulnerability, but the use of these methods has not led to a definitive solution, because some tools are too expensive to be distributed to all users and others are difficult to be employed by ordinary users [3].

2.3 Why not use advanced authentication technology?

Various organizations have conducted surveys on this question. In one example, the Information-technology Promotion Agency (IPA) [27], which is a Japanese government agency, pointed out that in addition to the costs involved with adopting an advanced authentication technology, many service organizations expressed concerns that adding additional measures might result in a decline in their service usage rate. Hence, when considering the burdens placed on users, it is often difficult for service providers to transfer to new methods.

However, a private research institute [11] in Japan mentions a contradictory point. Before choosing an Internet banking service, user priorities are as given below:

1st: Low fees 51.4%, 2nd: Enhanced security measures 47.4%, 3rd: Business soundness 46.0%

From these figures, it appears that while users have serious concerns about security of their service providers, 80% place higher importance on user-friendliness when choosing a service, and may even choose another provider if there are difficult hurdles, such as the need to install hardware tokens.

2.4 Society must change completely and drastically

It is clear that the ID/password authentication method is reaching the limits of its utility, primarily because password use is dependent on user memory, and thus tends to be vulnerable. One way to solve this problem is to improve user literacy, but that is a very long-term project. Additionally, systems based on encryption keys require specialized software and hardware that have not become widespread, and also face issues related to key-logging attacks.

Furthermore, even though the phrase “highly secure and convenient authentication is required” has been heard for more than 20 years, there have been no significant changes. Thus, it is clear that something else is required, in addition to high-level security and convenience.

New attacks occur all the time. For example, in the future, it is expected that fingerprints will be collected from photographs.

3 Social background

The current social background is the result of numerous changes. Unlike the early days of the Internet, numerous high-speed networks have now been completed and user devices have become much more sophisticated.

3.1 User devices have changed

The Internet users of today have access to several new devices that were rare just 10 years ago. Those devices have become increasingly sophisticated, and it is particularly noteworthy that vast numbers of users now possess smartphones that have very advanced specifications. Japan’s Ministry of Economy, Trade and Industry notes that in mid-2014 smartphones had overtaken personal computers as the device most commonly used for EC [21]. One example was provided by the statistics of Start Today Co., Ltd., which is one of the largest EC companies in Japan, in their published figures for

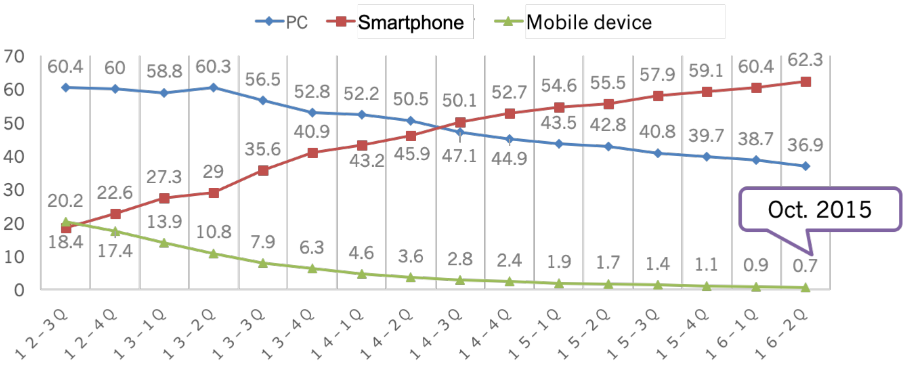

Figure 3: Recent Trend for Shipping ratio by Devices

“Shipping ratio by device”, which were extracted from the market trends in FY2014 Infrastructure Development [20] [19]. These are shown in figure 3.

Zenith mentions recent trend [38].

3.2 Cashless society

The concept of a cashless society is now becoming more widely accepted [39]. As a means to provide an appropriate infrastructure for credit card payments, 100% of all credit card companies switched to IC cards by 2020. To realize a cashless society, providing infrastructure for credit card payments has become essential [34] [22]. The reason why a cashless society is gaining importance is because cashless media are more resistant to attack than the security technologies available for physical media, such as printed banknotes. One recent manifestation of that trend is the fact that high-value banknotes are now being scrapped by several countries.

4 Before looking at “behavior” as a fourth factor authentication technology

Security experts tend to seek “perfect security,” and within that, “convenience.” However, it is questionable if this is the ideal way to build a large infrastructure. First, consider the credit card world, where providers focus on the importance of cost-effectiveness and where user acceptance is also important. For low-value payments, the switch to cards that do not require a signature depends on the card type, and the issue of fraudulent use is covered by insurance. By accepting the inevitability of some fraudulent use, and thus reducing the cost of system introduction, overall total costs are reduced [34].

It is expected that the increasing security provided by this outlook will result in cheaper insurance premiums and improved user convenience.

4.1 Personal authentication

Digital authentication is defined by NIST as follows [10]: “Digital authentication establishes that a subject attempting to access a digital service is in control of one or more valid authenticators associated with that subject’s digital identity. For services in which return visits are applicable, successfully authenticating provides reasonable risk-based assurances that the subject accessing the service today is the same as that which accessed the service previously.”

The above definition was created in 2006 and has been updated repeatedly [4]. The latest version was published in 2017 [10].

By the time the SP800-63 standard was created, the term three-factor authentication (3FA) had already entered common use. The three elements of this authentication type are said to be something you know, something you have, and something you are.

4.2 Risk-based authentication

Another recent trend is risk-based authentication methods, which are now in use by several EC sites. In these methods, access attempts are judged to be usual or unusual based on information such as the device operating system (OS), browser Internet Protocol (IP) location, and similar related factors [32]. Based on the risk assigned, users can expect to receive an email asking, ”Have you performed this activity recently?”

5 Fourth factor authentication

While the use of intelligent devices such as smartphones is continuing to spread rapidly, most service providers continue to rely on ID/password authentication methods, and the modernization of authentication technology is currently recognized as an ongoing challenge for society. However, authentication technology that uses information and communications technology (ICT) to identify people based on information about their habits already exists. In such methods, by using information obtained from smartphones and wearable devices, individuals can be authenticated without requiring the user to carry out any specific authentication operations. Focusing on convenience makes it possible to increase users and create a safer society.

5.1 Behavior as a factor

Behavior authentication factors that have been proposed for use to date include gait recognition [15] [26] [25] and keystroke authentication [2]. Other approaches focus on mobile motion [9] and touch gestures [6]. These schemes have been regarded as developments in the field of biometrics. Also, risk-based authentication uses behavior factor such as user’s device or shopping behaviour [32].

Here, we would like to point out a potential behavior factor that is separate from biometrics, that is the “concept of time”.

5.1.1 Definition: the time concept as a behavior factor

Here, we consider a situation in which user A wants to be provided a service S by a service provider B at a time t. In such a case, S needs to ensure that A has a right r to be provided the service. If S is a kind of exchange, the result is a barter. This is the same process as the previous authentication, the only difference being that S checks the r of A.

Currently, most e-commerce services are not exchange programs. When A begins viewing a webpage at t_0, checks his or her interests at t_1, and then adds purchases to his or her individual cart at t_2, it can take a significant amount of time. Then, A goes to the checkout page at t_3 and provides their certificate to B for personal authentication.

However, in recent risk-based authentication schemes, B checks behavior from t_0 to t_3. If B can identify any suspicious behaviors, B will inform A at t_3. This concept is very similar to the implicit authentication scheme [13]. Also, we say the same applies to the techniques covered in section5.1.

Here, the fourth factor is considered to be changing the authentication status.

5.1.2 Security Discussion

Introducing the new concept of time makes security discussions more difficult.

”Something you know”, such as ID/password techniques, and ”Something you have” use the discussions about amount of information [4]. However, it is difficult to define a dictionary attack only by mathematical theory, but also there are also new types of attacks such as password list attacks.

"Something you are" uses FRR, False Rejection Rate, and FAR, False Acceptance Rate. "Something you do" might use same discussion but there are some problems to use FRR and FAR. Unlike other methods, this method is forced to adopt a method that corrects fluctuations, and it is obliged to make ambiguous acceptance. The FRR must be to increase. To solve these problems, a new approach different from FRR is necessary, which is distinguishability.

5.2 Using life patterns for behavior authentication

There are several approaches for personal authentication techniques using life patterns.

5.2.1 Life pattern analysis

There have already been some studies on personal authentication methods that utilize lifestyle patterns. For example, Tang et al. used location information captured by the Global Positioning System (GPS) [33]. Authentication methods using content posted on social networking services (SNSs), rather than information obtained by sensors, have also been investigated. For example, Sultana et al. [29] argued that social interactions provide information on unique individual behavioral patterns. In their study, in which they analyzed online social context data on 241 Twitter users, they concluded that social behavioral biometric features contain properties such as uniqueness, stability, and recognition accuracy for frequent and non-frequent online social networking user sets.

Another study is based on machine learning techniques and and thinking patterns. In [14], they discussed the difference between what people think and how people behave.

5.2.2 Multifactor authentication system using lifestyle patterns

In a separate study, Fridman et al. [7] conducted an authentication experiment using multiple factors. More specifically, they combined four biometric behavioral modalities: text entered via soft keyboard, application usage, history of websites visited, and the physical location of the device. Similarly, we have conducted various data collection experiments using device information captured by Wi-Fi Sensors [17] [18], as well as experiments using wearable device sensors instead of smartphones [30]. The latter experiments were aimed at realizing an authentication method that utilized user activity information. Also, there is one study as a multiple authentications with using thinking pattern [23].

Based on the results of these experiments, we have developed an authentication system that utilizes behavior history information, including user purchase histories, location information, information from wearable devices, and other such data [16]. It should be noted that the system's scope is much wider than just authentication but for this paper, we will concentrate on using the system for behavior authentication. One of the unique features of this authentication system is that it requires multifactor authentication, in which a more accurate and user-friendly verification is achieved by combining multiple authentication factors. Figure 4 shows an overview of the entire system. Here, it can be seen that personal data from the (left) user side is collected together with user data extracted from the (right) server side. The multifactor authentication system in the middle then uses various key technologies such as AI based data analysis and modeling to authenticate the user via his or her personal information.

6 Discussion

Although the proposed fourth authentication factor needs to provide security, several issues remain. These will be discussed below.

6.1 Privacy problem

As authentication methods become more sophisticated, privacy problem issues are becoming increasingly important. Of particular interest here is the fact that the proposed fourth authentication factor has more problems than the third authentication factor, which is biometrics.

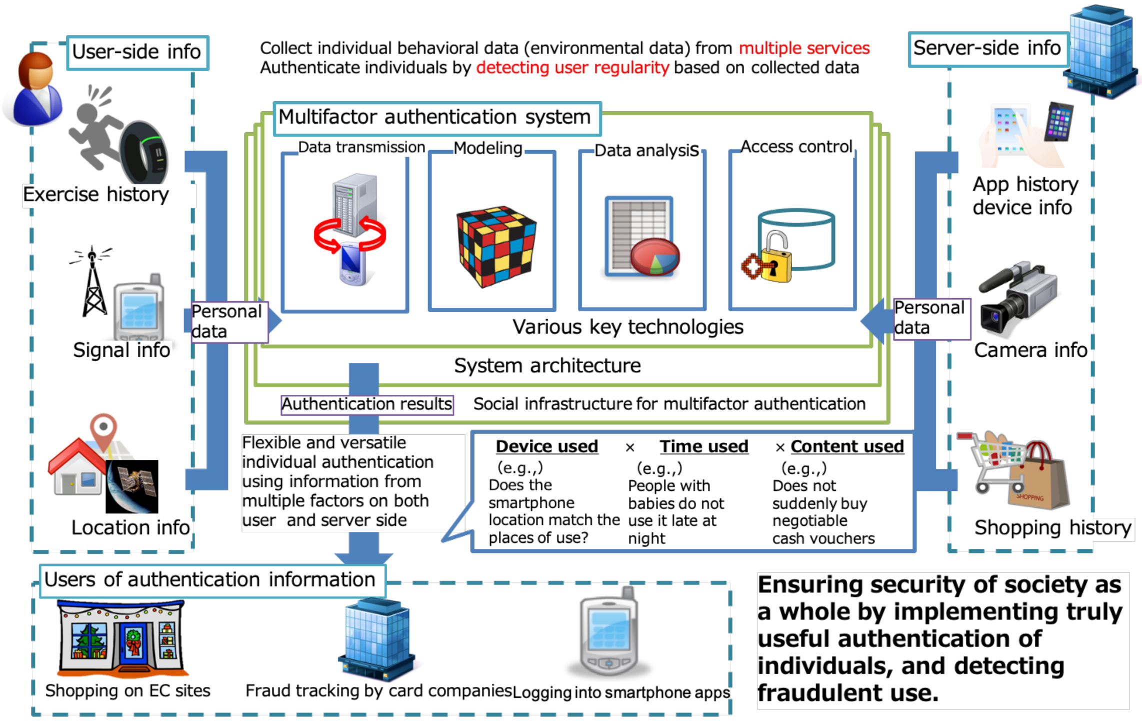
User-side info
Collect individual behavioral data (environmental data) from multiple services
Authenticate individuals by detecting user regularity based on collected data
Server-side info
Exercise history
Signal info
Location info
Multifactor authentication system
Data transmission
Modeling
Data analysis
Access control
Personal data
Various key technologies
Personal data
System architecture
Authentication results
Social infrastructure for multifactor authentication
App history device info
Camera info
Shopping history
Flexible and versatile individual authentication using information from multiple factors on both user and server side
Device used
×
Time used
×
Content used
(e.g.,) Does the smartphone location match the places of use?
(e.g.,) People with babies do not use it late at night
(e.g.,) Does not suddenly buy negotiable cash vouchers
Users of authentication information
Shopping on EC sites
Fraud tracking by card companies
Logging into smartphone apps
Ensuring security of society as a whole by implementing truly useful authentication of individuals, and detecting fraudulent use.

Figure 4: The overview about behaviour factor data structure

Everybody agrees that the issue of balance between security and privacy is a major concern. As one example, it must be acknowledged biometric data cannot be changed repeatedly.

Another issue can be seen in an examination of the surveillance cameras installed throughout the city of London [36], England, where intense discussions took place before, during, and even after the installation of the system. Now, when police observers or persons from other monitoring organizations witness strange or unsafe behaviors via such cameras, they can issue cautions, instructions, or commands to those involved via loudspeakers mounted on nearby utility poles. Although there are fears that a surveillance society has been created, it is also true that security was improved by installing those cameras.

Approaching the issue from another angle, we note that many methods have been proposed to solve these kinds of privacy protection problems, and the results of several access control studies have already been put into practical use. In the field of biometrics, some methods already exist to safeguard the biometric data used [24].

It is clear that the issues to be discussed will change with the times.

6.2 Robustness

Behavior-based 4FA can be considered a way of realizing robust multifactor-multimethod authentication. More specifically, data extracted from habitual use behaviors are used in the authentication process. These schemes are based on the effective use of sensor data. The authentication factors are extracted from habitual behavior of users.

For a variety of reasons, these schemes can be expected to provide the basis for a new robust authentication infrastructure. As one example, they can facilitate flexible vulnerability responses that could be effective measures against biometric information forgery attempts. Additionally, since the user behavioral characteristics, the devices operated, and the environments in which they are used will vary from user to user, an abundance of available factor combinations have the potential to provide a basis for potential safety improvements. Another advantage of the scheme is that it does not depend on user literacy.

6.3 Toward a new era of security measures

Up until now, the implementation of a groundbreaking technique has always been necessary for applying a security measure at a certain point during the authentication process. It is felt that designers should focus on measures appropriate to user acceptance and risk, as well as the realization of "total security" systems that combine existing security measures with an eye towards areas other than IT systems, such as security guards and insurance.

7 Conclusion

As an accompaniment to existing 4FA models, the use of behavior as an authentication technique is considered promising not only in regards to security but also usability. Accordingly, it is believed that the use of behavior as a fourth factor for various services should be seriously considered more for its ability to help secure a safe and secure society than as just a means of efficiency. In the future, this field will require significant developments, especially in terms of multifactor authentication.

References

[1] Leonard Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. In *IEEE, 20th Annual Symposium on Foundations of Computer Science (SFCS 1979)*, pages 55–60, Oct 1979.

[2] Francesco Bergadano, Daniele Gunetti, and Claudia Picardi. User authentication through keystroke dynamics. *ACM Trans. Inf. Syst. Secur.*, 5(4):367–397, 2002.

[3] Christina Braz, Ahmed Seffah, and David M'Raihi. Designing a trade-off between usability and security: A metrics based-model. In *Human-Computer Interaction – INTERACT 2007*, pages 114–126. Springer Berlin Heidelberg, 2007.

[4] William E. Burr, Donna F. Dodson, and W. Timothy Polk. Nist special publication 800-63: Electronic authentication guideline. *https://csrc.nist.gov/csrc/media/publications/sp/800-63/ver-10/archive/2004-06-30/documents/sp800-63-v1-0.pdf (accessed 2020-01-27)*, 2004.

[5] Japan Cabinet Office. society 5.0. *https://www8.cao.go.jp/cstp/english/society5_0/index.html (accessed 2020-01-27)*, 2019.

[6] Tao Feng, Ziyi Liu, Kyeong-An Kwon, Weidong Larry Shi, Bogdan Carbunar, Yifei Jiang, and Nhung Nguyen. Continuous mobile authentication using touchscreen gestures. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, pages 451–456, 2012.

[7] L. Fridman, S. Weber, R. Greenstadt, and M. Kam. Active authentication on mobile devices via stylometry, application usage, web browsing, and gps location. *IEEE Systems Journal*, 11(2):513–521, June 2017.

[8] Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. In *Spanish Workshop on Biometrics, SWB 2007*, pages 1–8, 06 2007.

[9] S. Milton Ganesh, Paul Vijayakumar, and L. Jegatha Deborah. A secure gesture based authentication scheme to unlock the smartphones. *2017 Second International Conference on Recent Trends and Challenges in Computational Models (ICRTCCM)*, pages 153–158, 2017.

[10] Paul A. Grassi, Michael E. Garcia, and James L. Fenton. Nist special publication 800-63-3: Digital identity guidelines. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf (accessed 2020-01-27)*, 2017.

[11] Fujitsu Research Institute (in Japanese). Survey on attitudes to security in internet banking. *https://www.ffri.jp/news/release_20131205.htm (accessed 2018-05-20)*, 5 December, 2013.

[12] My Navi News (in Japanese). Yahoo! japan introduces a login method that does not require password input. *https://news.mynavi.jp/article/20170420–a220/ (accessed 2017-10-27)*, 20 April 2017.

[13] Markus Jakobsson, Elaine Shi, Philippe Golle, and Richard Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, HotSec'09, page 9, USA, 2009. USENIX Association.

[14] B. Johnson, T. Maillart, and J. Chuang. My thoughts are not your thoughts. In *Proc. ACM Intl. Joint Conf. on Pervasive and Ubiquitous Computing (UbiComp 2014)*, pages 1329–1338, 2014.

[15] A. Kale, A. Sundaresan, A. N. Rajagopalan, N. P. Cuntoor, A. K. Roy-Chowdhury, V. Kruger, and R. Chellappa. Identification of humans using gait. *IEEE Transactions on Image Processing*, 13(9):1163–1173, Sep. 2004.

[16] Ryosuke Kobayashi. Large scale poc experiment with 57,000 people to accumulate patterns for lifestyle authentication. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy*, CODASPY 2019, Oct 2019.

[17] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi. A behavior authentication method using wi-fi bssids around smartphone carried by a user. *IEEE, 2015 Third International Symposium on Computing and Networking (CANDAR)*, pages 463–469, 2015.

[18] Ryosuke Kobayashi and Rie Shigetomi Yamaguchi. One hour term authentication for wi-fi information captured by smartphone sensors. *2016 International Symposium on Information Theory and Its Applications (ISITA)*, pages 330–334, 2016.

[19] Start Today Co. Ltd. Ir data 2015. *http://www.starttoday.jp/wp-content/uploads/2015/10/CFM2.0.pdf (accessed 2017-10-27)*, 1 May 2015.

[20] Start Today Co. Ltd. Ir data 2014. *http://www.starttoday.jp/wp-content/uploads/2014/04/ir20140430-jp.pdf (accessed 2017-10-27)*, 30 April 2014.

[21] Trade Ministry of Economy and Japan Industry. Japan's information-based economy and society. *http://www.meti.go.jp/policy/it_policy/statistics/outlook/h26report.pdf (accessed 2017-10-27)*, 1 May 2015.

[22] Trade Ministry of Economy and Japan Industry. Action plan 2019 for the consolidation of security measures for credit card transactions formulated. *https://www.meti.go.jp/english/press/2019/0304_003.html (accessed 2020-01-27)*, March 4, 2019.

[23] T. Mochida and M. Inamura. Personal authentication method based on human preference prediction using machine learning. In *Proc. Intl. Joint Conf. on e-Business and Telecommunications (ICETE 2018)*, volume Vol.1, pages 297–304, 2018.

[24] Takao Murakami, Ryo Fujita, Tetsushi Ohki, Yosuke Kaga, Masakazu Fujio, and Kenta Takahashi. Cancelable permutation-based indexing for secure and efficient biometric identification. *IEEE Access*, 7:45563–45582, 04 2019.

[25] Thanh Trung Ngo, Yasushi Makihara, Hajime Nagahara, Yasuhiro Mukaigawa, and Yasushi Yagi. The largest inertial sensor-based gait database and performance evaluation of gait-based personal authentication. *Pattern Recognition*, 47(1):228 – 237, 2014.

[26] Liu Rong, Zhou Jianzhong, Liu Ming, and Hou Xiangfeng. A wearable acceleration sensor system for gait recognition. In *2nd IEEE Conference on Industrial Electronics and Applications ICIEA 2007*, pages 2654 – 2659, 06 2007.

[27] Information Promotion Agency (in Japanese) Security Center. Field survey of online user authentication methods. *https://www.ipa.go.jp/security/fy26/reports/ninsho, (accessed 2020-01-27)*, 5 August, 2014.

[28] Shiuh-Jeng Wang, P. S. Chen, and Ya-Chi Lin. Log-in authentication based on locating centers of a triangle. In *2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. TENCOM '02. Proceedings.*, volume 1, pages 125–128 vol.1, Oct 2002.

[29] M. Sultana, P. P. Paul, and M. L. Gavrilova. User recognition from social behavior in computer-mediated social context. *IEEE Transactions on Human-Machine Systems*, 47(3):356–367, June 2017.

[30] Hiroya Susuki and Rie Shigetomi Yamaguchi. Cost-effective modeling for authentication and its application to activity tracker. In *International Workshop on Information Security Applications, WISA*, pages 373–385, 2015.

[31] Symantec. Report on the results of an awareness survey on personal and corporate password management. *https://www.digicert.co.jp/welcome/pdf/password_management_survey.pdf*, 2013.

[32] Symantec. Simantec vip. *https://vip.symantec.com (accessed 2020-01-27)*, 2017.

[33] Yujin Tang, Nakazato Hidenori, and Yoshiyori Urano. User authentication on smart phones using a data mining method. *2010 International Conference on Information Society*, pages 173–178, 2010.

[34] Timestaff. How do i fix a suspicious charge on my credit or debit card? *https://money.com/collection-post/suspicious-charge-credit-debit-card/ (accessed 2020-01-27)*, MAY 26, 2014.

[35] Jeremy Wagstaff and Malathi Nayak. Pple bashers just don't get it: That new fingerprint sensor takes biometrics mainstream! *Sep. 12, https://www.businessinsider.com/apple-fingerprint-sensor-biometrics-2013-9, (accessed 2020-01-27)*, 2013.

[36] Matthew Weaver. Uk public faces mass invasion of privacy as big data and surveillance merge. *The Guardian News Paper, https://www.theguardian.com/uk-news/2017/mar/14/public-faces-mass-invasion-of-privacy-as-big-data-and-surveillance-merge (accessed 2020-01-27)*, 14 March 2017.

[37] Elizabeth Weise. Amazon set to open its grocery store without a checkout line to the public. *USA Today, https://www.usatoday.com/story/tech/news/2018/01/21/amazon-set-open-its-grocery-store-without-checkout-line-public/1048492001/ (accessed 2020-01-27)*, 21th of Jan. 2018.

[38] Zenith. Smartphone penetration to reach 66% in 2018. *https://www.zenithmedia.com/smartphone-penetration-reach-66-2018 (accessed 2020-01-27)*, 2018.

[39] RUI ZHONG. China can't afford a cashless society. *https://foreignpolicy.com/2018/09/11/china-cant-afford-a-cashless-society/ (accessed 2020-01-27)*, 11th, Nov. 2018.