Pattern Recognition Letters
journal homepage: www.elsevier.com

Exploring Touch-based Behavioral Authentication on Smartphone Email Applications in IoT-enabled Smart Cities

Wenjuan Li[a,b], Weizhi Meng[a,**], Steven Furnell[c]

[a] *Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark*
[b] *Institute of Artificial intelligence and Blockchain, Guangzhou University, China*
[c] *Faculty of Science, University of Nottingham, UK*

ABSTRACT

The Internet of Things (IoT) allows various embedded devices and smart sensors to be connected with each other, which provides a basis for building smart cities. The IoT-enabled smart city can greatly benefit people's daily lives, where smartphone is one of the most widely used IoT devices. For example, people can use the phone to check their financial account, store personal data and communicate with peers. Thus it is very important to safeguard the phones from unauthorized access. To complement traditional textual passwords, touch behavioral authentication has attracted much attention while it is still a challenge on how to build a robust scheme in practice. This is because users' touch actions are often dynamic and hard to model. For this challenge, previous work has proved that touch actions could become consistent when users interact with social networking applications. Motivated by this observation, in this work, we perform a study to investigate users' touch behavior within Email applications on smartphones (with Email being one of the most important and widely used means in connecting with others). The study results with 60 participants validate the former observation that users' touch behavioral deviation can be greatly decreased when they play Email applications.

1. Introduction

The goal of a smart city is to deploy sustainable solutions based on information and communication technologies (ICT) to benefit people's living (Shen et al., 2019). A main feature of smart cities is the integration of various connected devices and objects. As such, one can consider the Internet of Things (IoT) as the basis of building a smart city, which enables various Internet-enabled devices and smart sensors to be connected with each other. A report from Gartner predicted that the enterprise IoT market may grow up to 5.8 billion by the end of 2020 (Gartner, 2019).

Currently, smartphones are the most widely used IoT devices, where users can store personal data on their phones and use such devices to access their financial accounts and maintain the connection with their peers. A report from Deloitte indicated that more than 84% of European people having a smartphone, and the rate reaches 94% for Luxembourg, Norway and Spain (Deloitte, 2018). Due to the importance of smartphones, they have become a major target for cyber-criminals. A report from eMarketer highlighted that Denmark has the highest smartphone penetration rate of around 77% in 2017 (eMarketer, 2017). Previous studies like (Barra et al., 2018, 2019; Ometov et al., 2019) also figured out that authentication mechanism is important for mobile devices under IoT and cloud environments. Hence there is an emerging need to protect such mobile devices from unauthorized access.

Up to now, textual passwords (e.g., passcode) are still the most prevalent authentication method on smartphones. However, such authentication techniques suffer from many known disadvantages. For example, users find it difficult to remember a long and random passcode due to the long-term memory limitation (Meng et al., 2016a). Instead, users may choose a weak password, making the authentication easily compromised by various guessing attacks (Schechter et al., 2019; Dell'Amico and Filippone, 2015). In addition, the password entry process on smartphones can be leaked under smudge attacks (Cha et al.,

[**] Corresponding author: Tel.: +45 45253068;
e-mail: weme@dtu.dk (Weizhi Meng)

This article was published in Pattern Recognition Letters, Vol. 144, W.Li, W.Meng and S.Furnell, "Exploring touch-based behavioral authentication on smartphone email applications in IoT-enabled smart cities", pp35-41, Copyright Elsevier (2021)

2017) and charging attacks (Meng et al., 2015a, 2019a). Also, after a successful login, traditional password-based systems cannot continuously verify the current users.

To complement the textual passwords, behavioral authentication has been developed that verifies users according to their behavioral features like touch behavior on mobile devices (Wu et al., 2020). For example, (Shen et al., 2016) provided an authentication scheme based on touch-interaction operations including sliding operation and tapping operation, with features such as position, angle, time, velocity, etc. (Meng et al., 2016b) described TMGuard, a touch movement-based security mechanism to enhance the unlock mechanism by validating users' touch movement during the input of unlock patterns. (Buriro et al., 2018) introduced DIALERAUTH, which can authenticate users based on how they enter a 10-digit string. This scheme particularly models the timing differences among touch strokes and micro-movements of their hand.

Though many touch behavioral authentication schemes are proposed, it is still a challenge to design a robust scheme for practical usage. This is mainly because users' touch actions are dynamic and hard to build an accurate model. It is found that the error rate in (Shen et al., 2016) is ranged from 1.72% and 9.01%, but they indicated that authentication accuracy can be improved when users do some specific things like web surfing. With the similar purpose, (Meng et al., 2019b) proposed SocialAuth, a touch behavioral authentication scheme based on users' touch habits on social networking applications. They validated the observation and found that touch behavioral deviation could be greatly reduced even after several weeks.

In the literature, there are many studies investigating the use of behavioral authentication in IoT, but few studies focusing on a smart city scenario. Intuitively, biometrics can be widely applied for authenticating users' entities when they move around different smart environments. With the rapid growth of IoT devices, there is a trend on discussing how to design behavioral authentication schemes in the context of smart cities. Motivated by the prior research like (Meng et al., 2019b), our main purpose in this work is to explore users' touch behavior on smartphone-based email applications, as this type of application is widely used by phone users. Our contributions can be summarized as below.

- Similar to SocialAuth in (Meng et al., 2019b), we adopt the same feature set in this work, including 22 features extracted from three main touch interactions such as single touch, touch movement and multi-touch. Our goal is to explore the deviation of users' touch behavior when they play Email applications on smartphones.

- In our user study, we collect the data from a total of 60 participants. We mainly consider three scenarios: 1) free task, 2) Email usage task, and 3) SocialAuth. More specifically, we analyze all touch data in the first scenario, while only considering the touch actions during the use of Email applications and social networking applications in the second and the third scenario, respectively.

- We test five typical supervised learning classifiers and the results indicate that SVM can outperform others with an average error rate (AER) of around 2.9%, which is similar but slightly better than that of SocialAuth. Our results validate that users' touch actions on smartphones could become even more stable when using Email applications.

The remainder of the paper expands upon the background to the research, and the specifics of the approach and findings in this study. Specifically, section 2 reviews relevant research studies on touch behavioral authentication on mobile devices. Section 3 introduces authentication architecture, touch gestures and the extracted features. Section 4 describes a user study with 60 participants and analyzes authentication performance regarding authentication accuracy and long-term performance. We discuss some challenges in Section 5 and conclude this work in Section 6.

2. Related Work

Touch-based behavioral authentication mainly verifies users via their touch actions. With the rapid development of IoT, touchscreen has become more popular than before. In an IoT-enabled smart city, users are supposed to complete various tasks by interacting with touchscreen sensors and devices. Currently, smartphone is the most commonly used IoT device that facilitates users' daily lives, e.g., it is convenient to purchase online with mobile payment, and to handle various personal or corporate Emails.

In the literature, different forms of touch behavioral authentication schemes are developed. (Meng et al., 2012) provided an early study to investigate the feasibility of authenticating users based on their touch actions. They selected 21 features by considering the similarities and differences among touch actions, keystroke dynamics and mouse dynamics. With a combined classifier of neural network and Particle Swarm Optimization (PSO), they achieved an error rate of around 3%. Then, (Frank et al., 2013) introduced a scheme called Touchalytics, which includes 30 features by considering sliding horizontally and vertically. They explored the authentication performance within one session and multiple sessions. An equal error rate (EER) of around 4% was achieved. The results from the above studies are promising but need to be validated in recent years, as there are much more applications available than before, which may affect users' touch habit.

In addition, Touchalytics only focused on single-touch gestures, and needed to be extended to multi-touch actions. For this issue, (Sae-Bae et al., 2014) introduced a scheme based on multi-touch actions of five fingers, with 22 multitouch gestures that were computed by using pair-wise Euclidean distances. In the user study, their results showed an EER of 7.88% on average. The main limitations are the small number of participants and the unstable authentication accuracy.

To enhance the authentication performance, one possible solution is to design combined behavioral authentication schemes. (Meng et al., 2016b) combined Android unlock mechanism with touch movement-based authentication. They designed a scheme called TMGuard that can validate a user based on both touch movement and input pattern. They identified that touch actions for inputting a pattern would become more stable after

Table 1. Performance of behavior-based schemes in the litreature.

Research Work	Performance
(Meng et al., 2012)	3% (Average Error Rate)
(Frank et al., 2013)	4% (Equal Error Rate)
(Sae-Bae et al., 2014)	7.88% (Equal Error Rate)
(Song et al., 2017)	5.84% (Equal Error Rate)
(Buriro et al., 2018)	85.77% (True Acceptance Rate)
(Meng et al., 2018)	2.4% (Average Error Rate)
(Meng et al., 2019b)	3.1%-3.7% (Average Error Rate)

more trials. (Song et al., 2017) introduced a scheme of verifying a user based on the combination of geometry information and touch behavior. This scheme could reach an EER of 5.84% if considering 5 samples during the training. (Buriro et al., 2018) combined PIN with single touch-based authentication. They designed a scheme called DIALERAUTH, which verifies users when they enter a 10-digit string. They used one-class Multilayer Perceptron (MLP) and presented a True Acceptance Rate (TAR) of 85.77% for legitimate users.

Another promising solution of authentication enhancement is to authenticate users when they perform certain tasks. (Shen et al., 2016) designed a touch behavioral authentication scheme by considering some scenarios when users perform sliding and tapping operations on the screen. (Meng et al., 2018) proposed TouchWB, which authenticates users based on their touch gestures on browsing webpages. With 48 participants and a hybrid classifier of PSO-RBFN, they could reach an AER of 2.4%. Similarly, (Chen et al., 2020) also explored the authentication based on browsing behavior, and showed the feasibility. Then (Meng et al., 2019b) proposed SocialAuth, by validating users when they play social networking applications. These research studies proved that users' touch actions could become easier to model than free tasks. Their study with 50 participants indicated that touch behavioral deviation could be reduced even after a long-term period. Their SVM classifier could achieve an average error rate of 3.1% and 3.7% before and after two weeks. Table 1 summarizes the performance of behavior-based schemes in the literature. Some additional work regarding behavioral authentication can refer to surveys like (Gomez-Barrero and Galbally, 2020; Liang et al., 2020; Sundararajan et al., 2019; Meng et al., 2015b; Teh et al., 2016).

Biometrics in the context of smart city. Currently, IoT has been gradually adopted by many organizations, enabling objects to be connected remotely. That is, users have the capability to control different things via Internet, such as electronic furniture, electronic product, electronic kitchenware and more. In this case, there is a need to authenticate legitimate users from the view of security.

Biometrics like behavioral biometrics provide a promising way of implicitly authenticating users. For instance, (Marsico et al., 2019) introduced a biometric authentication scheme based on gait dynamics in a smart city. This approach can authenticate users based on the smartphone sensors and with less computational burden. Currently, smartphones have become a major tool used in IoT and smart environments (e.g., smart home, smart city), how to design a secure and robust biometric authentication scheme receives much attention from both academia and industry.

3. Touch Behaviorial Scheme based on Email Applications

This section introduces the behavioral authentication scheme based on machine learning on smartphones including touch gestures, extracted features and session identification.

3.1. Authentication Scheme

Touch-based behavioral authentication continuously verifies a user's entity, which can complement existing authentication methods. Figure 1 illustrates the workflow of touch behavioral authentication scheme in this work, including data processing, touch gesture modelling and touch gesture matching.

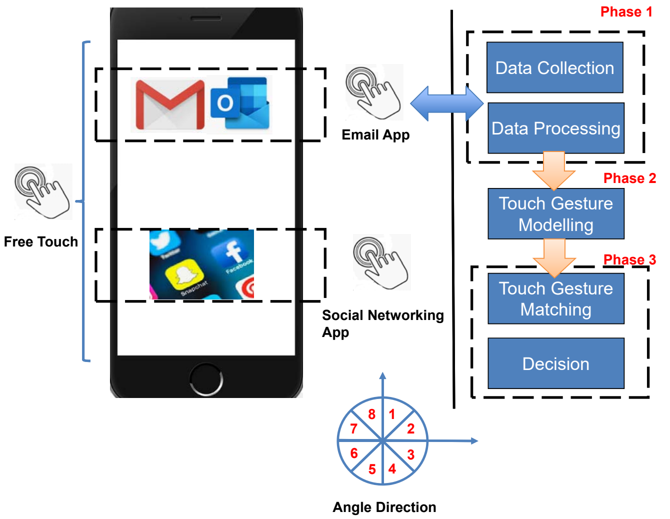

Fig. 1. The workflow of touch behavioral authentication system.

- **Phase 1.** This phase mainly contains *data collection* with the aim of gathering / recording users' touch actions, and *data processing* that filters out noise / unwanted data and extracts touch-related features.
- **Phase 2.** This phase applies machine learning classifiers to model users' touch behavior based on the selected features. In the literature like (Shen et al., 2016; Meng et al., 2019b), supervised learning has been widely used such as K-Nearest-Neighbors (KNN), Support Vector Machine (SVM), and Backward-Propagation Neural Network (BPNN).
- **Phase 3.** This phase aims to compare the current touch behavior with the pre-built normal touch behavior template, generate an alarm if a significant deviation is found (based on the selected threshold), and ultimately decide whether the user is legitimate or not.

3.2. Touch Features and Session Identification

Similar to previous studies (Meng et al., 2012, 2019b), this work also considers the same touch gestures, features and session identification, in order to facilitate the performance comparison. We consider the following major touch gestures.

- **Single Touch:** this kind of touch action refers to user interactions with the touchscreen using only one finger, and no movement during the touch action. The key example here is a screen tap.
- **Touch Movement:** this kind of touch action refers to instances in which users move their finger(s) along the touchscreen, such as swipe, drag, flick, etc.
- **Multi Touch:** this kind of touch action refers to interactions with the touchscreen using more than one finger, such as pinch, zoom-in, zoom-out, and so on.

Touch Features. Similar to (Meng et al., 2012, 2019b), based on these touch gestures, we extract the following 22 touch features including *average touch movement speed per direction* (eight directions), *the fraction of touch movements per direction* (eight directions), *average single-touch time*, *average multi-touch time*, *the fraction of touch movements per session*, *the fraction of single-touch events per session*, *the fraction of multi-touch events per session*, and *touch pressure*. The angle directions can refer to Figure 1.

1) Average Touch Movement Speed per Direction. If we consider two points ($x1$, $y1$) and ($x2$, $y2$) along a touch movement, then we can calculate *touch movement speed* (*TMS*) and *angle direction* accordingly.

$$TMS = \frac{\sqrt{(x2-x1)^2+(y2-y1)^2}}{S2-S1}$$

$$\textit{Angle direction: } \theta = \arctan\frac{y2-y1}{x2-x1}, \theta \in [0, 360^{\circ}]$$

2) Fraction of Touch Movements per Direction. This means the distribution of touch movements (*FTM*) in each direction.

3) Average Single-Touch and Multi-Touch Time. This means the time difference between a touch press-down and touch release, where *AST* represents *average single-touch time* and *MT-T* represents *average multi-touch time*.

4) Fraction of Touch Action Events. This means the distribution of three touch gestures within a session, where *FTM* represents *the fraction of touch movements per session*, *FSTE* represents *the fraction of single-touch events per session*, and *FMTE* represents *the fraction of multi-touch events per session*.

5) Touch Pressure. This means the touch strength when users interact with touchscreen, where *ATP* represents *average touch pressure*. For example, some users may perform a tap on touchscreen very heavily, resulting in a higher pressure value. On the other hand, some users may provide a smaller pressure value.

Session Identification. This work applies typically supervised machine learning classifiers for profiling users' touch actions (including both touch gesture modelling and matching). Similar to previous work (Meng et al., 2012, 2019b), we adopt the same session identification, in which each session contains 120 touch gestures, with the aim of ensuring enough gestures can be collected for each session.

Comparison with similar studies. As compared with other work like (Frank et al., 2013; Sae-Bae et al., 2014; Buriro et al., 2018), this work uses a different feature set for behavior-based authentication. As compared with (Meng et al., 2019b), the feature set is similar, but the target behavior type is not the same. The previous work investigated users behavior when they use social networking application, while this work focuses on users' behavior when they use Emails. Nowadays, Emails are a popular and important communication solation, in which users have to handle many Emails per day. Hence we believe there is a need to study users' behavior during Email usage on smartphones, and validate the observations in (Meng et al., 2019b).

4. User Study

This section introduces a user study with 60 participants including the data collection platform, machine learning classifiers, study steps, and the obtained results.

4.1. Collection Platform

To facilitate the comparison with similar work like (Meng et al., 2019b), we collect the touch behavioral data by using a smartphone type - Google/HTC *Nexus One* with a 3.7 inch touch screen and a resolution of 480×800 px. The main advantage of this phone is researcher-friendly, where it is not difficult to customize the phone settings according to the requirements. We particularly restored the phone with a customized Android OS - *CyanogenMod* (`http://www.cyanogenmod.com/`). We then use a log reading application to record the touch-related information such as the coordinates x and y, the timing of touch actions, and the touch pressure.

4.2. Machine Learning Algorithms

Similar to previous work (Meng et al., 2019b), we adopted five popular and typical supervised classifiers, such as Decision tree (J48), Naive Bayes, Radial Basis Function Network (RBFN), Back Propagation Neural Network (BPNN) and Support Vector Machine (SVM). All these classifiers are extracted from an open-source machine learning tool called WEKA (`https://www.cs.waikato.ac.nz/ml/weka/`) with default settings to avoid implementation bias.

We mainly use two metrics to evaluate the authentication performance:

- False Acceptance Rate (FAR): indicates the rate that an impostor is erroneously classified as a legitimate user.
- False Rejection Rate (FRR): indicates the rate that a legitimate user is mistakenly classified as an imposter.

In practice, an expected classifier aims for both a small FAR and FRR, whereas a tradeoff is often made to balance these two metrics due to the dynamic changes of touch behavior.

Table 2. Participants' background in the user study.

Occupation	Male	Female	Age	Male	Female
Students	20	17	18 - 30	22	20
Business	3	3	31 - 40	5	3
Researchers	10	3	40 - 50	2	3
Senior citizen	3	1	Above	3	2

4.3. Study Steps

We recruited a total number of 60 regular phone users (including 27 females and 33 males, aged from 18 to 60 years) via online recruitment and colleague recommendation in the study. They make regular daily use of many applications on a smartphone. Table 2 summarizes the detailed background of participants like age and occupation, i.e., students, senior citizens, researchers and business people.

Each participant in this study could get an Android phone (Google/HTC Nexus One with the updated OS). This aims to ensure there is no hardware difference in data collection, in order to avoid some unexpected influence. At the beginning, we introduced the research purposes to all participants, i.e., how this platform would collect their touch-related data, and how we ensure the data privacy and security. In particular, we demonstrated that no private / personal data would be collected or leaked. Then, we seek an approval from each participating entities before the study.

In this study, we randomly divided all participants into two groups (with 30 participants in each group) as below:

- *Group-1.* We mainly analyze participants' touch behavior under Email application usage (Gmail and Outlook) and free task.
- *Group-2.* We mainly analyze participants' touch behavior under Email application usage (Gmail and Outlook) and under social networking application usage (WeChat, Facebook, Twitter and Instagram).

During the study, we encouraged all participants to use this phone in the same way of using their daily phones. For this purpose, similar to previous work (Meng et al., 2019b), we allowed participants to use the phone out of the lab, so that they can have more time in getting familiar with the phone and completing the data collection. Each participant in relevant group has to finish 30 sessions for each situation within four days.

The collected sessions are larger than that in (Meng et al., 2019b), and we believe it is a good number for achieving our purpose. We therefore collected a total of 900 sessions for each situation. All participants were given a $30 gift card after completing the study.

4.4. Result Analysis

In summary, there are 22 touch features in this work (refer to Section 3.2), such as *ATMS1*, *ATMS2*, *ATMS3*, *ATMS4*, *ATMS5*, *ATMS6*, *ATMS7*, *ATMS8*, *FTM1*, *FTM2*, *FTM3*, *FTM4*, *FTM5*, *FTM6*, *FTM7*, *FTM8*, *AST*, *MTT*, *FTM*, *FSTE*, *FMTE* and *ATP*. As previous work has proved the effectiveness of these features, this work mainly focuses on analyzing touch behavioral deviation, authentication accuracy, and long-term authentication performance (after two weeks).

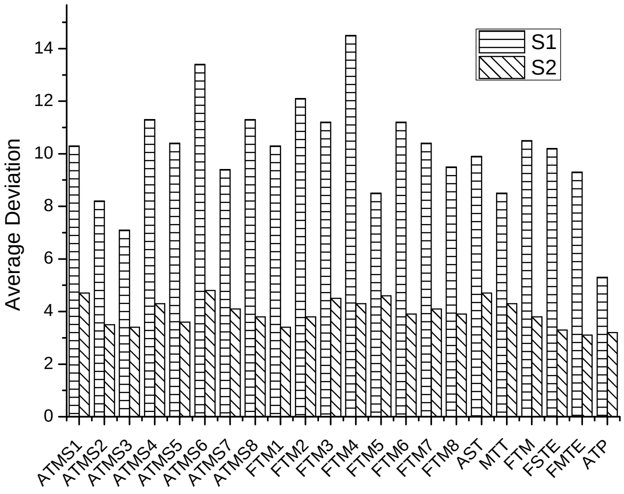

Fig. 2. The average behavioral deviation in Group-1.

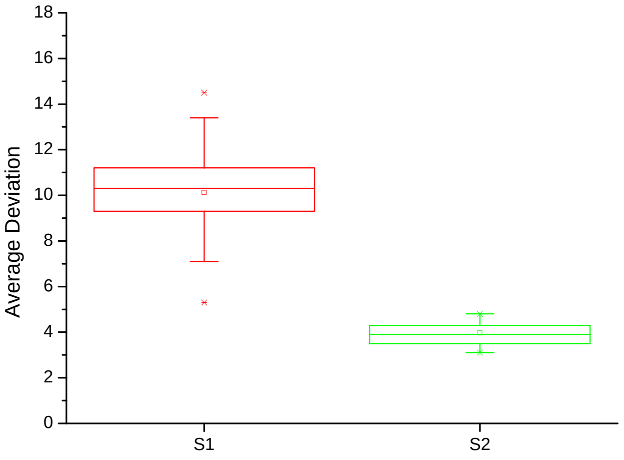

Fig. 3. The distribution of average deviation in Group-1.

Touch Behavioral Deviation. For Group-1, we explore the touch behavioral deviation under two scenarios: *S1* - free task and *S2* - Email application usage. For Group-2, we investigate the touch behavioral deviation under *S2* - Email application usage and *S3* - Social networking application usage.

- *Group-1.* Figure 2 depicts the average behavioral deviation in Group-1. It is found that the average deviation of each feature in *S2* is much smaller than that in *S1*. For instance, participants under *S1* made a deviation above 10 for ATMS1, ATMS4, ATMS5, ATMS6, ATMS8, FTM1, FTM2, FTM3, FTM4, FTM6, FTM7, FTM8, FTM and FSTE, whereas under *S2*, the relevant deviation ranged from 3.1 to 4.8. In addition, Figure 3 verifies that the average deviation values under *S2* are mostly only half or less than those under *S1*.
- *Group-2.* This group aims to compare the behavioral deviation when users play between Email applications and social networking applications. Figure 4 and Figure 5 depict the average behavioral deviation in this group, demonstrating that the average deviation in *S2* is generally better than that in *S3*. It is noticed that the deviation value for ATMS2, FTM4 and FSTE under *S3* is smaller than that under

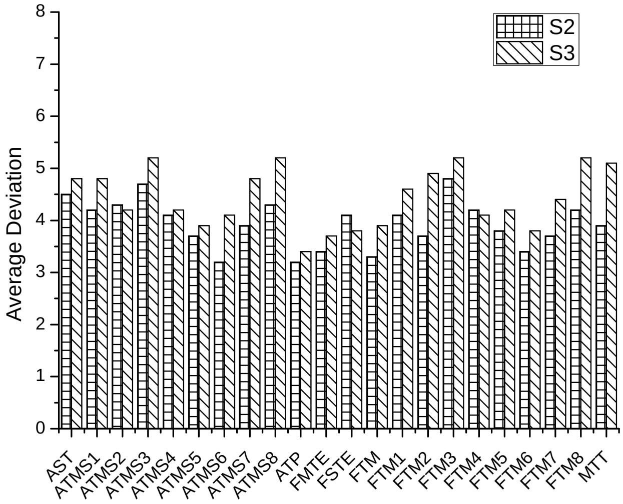

Fig. 4. The average behavioral deviation in Group-2.

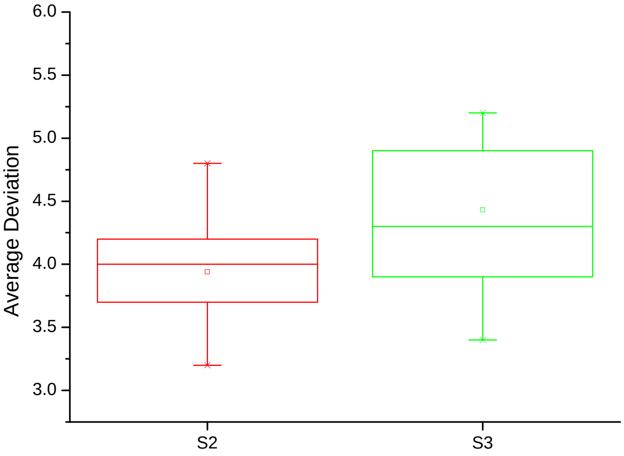

Fig. 5. The distribution of average deviation in Group-2.

S2, while most features under *S3* suffer from a higher deviation value compared to *S2*.

Overall, the obtained results in Group-1 validate the prior observation in (Shen et al., 2016; Meng et al., 2019b) that users' touch actions would become more stable under given custom tasks. In addition, the obtained results in Group-2 indicate that users' touch behavior is even more stable when they play Email applications on smartphones. This is mainly because social networking applications provide much more functions than Email applications, i.e., users mainly check, receive or send Emails under *S2*, while they can post messages and communicate with their peers under *S3*.

Authentication Accuracy. To study the performance of authentication with different classifiers, the same as (Meng et al., 2019b), we used 60% of the total sessions to train each classifier and used the rest for testing, with a 10-fold cross validation (provided by the WEKA platform). Table 3 and Table 4 describe the false acceptance rate (*FAR*), false rejection rate (*FRR*), and average error rate (*AER*) for two groups, respectively.

- *Group-1*. Table 3 shows that SVM classifier could achieve a better error rate than the other classifiers, i.e., the error rate of J48 and NBayes is above 10%. It achieved an AER of 6.34% and 2.79% under *S1* and *S2*, respectively. The rate under *S2* is less than half of the rate under *S1*. The results indicate that users' touch actions are more stable under a given task than free task, and can be used for designing a more robust authentication scheme.

Table 3. Authentication performance for different classifiers in Group-1.

S1	J48	NBayes	RBFN	BPNN	SVM
FAR (%)	21.43	17.36	10.83	9.23	6.24
FRR (%)	20.54	19.83	10.42	10.42	6.44
AER (%)	20.99	18.60	10.63	9.83	6.34
S2	J48	NBayes	RBFN	BPNN	SVM
FAR (%)	13.73	9.39	6.33	6.14	2.45
FRR (%)	12.35	11.42	6.82	6.63	3.12
AER (%)	13.04	10.41	6.58	6.39	2.79

Table 4. Authentication performance for different classifiers in Group-2.

S2	J48	NBayes	RBFN	BPNN	SVM
FAR (%)	14.23	11.42	7.53	6.78	3.08
FRR (%)	13.22	10.23	7.23	7.16	2.95
AER (%)	13.73	10.83	7.38	6.97	3.02
S3	J48	NBayes	RBFN	BPNN	SVM
FAR (%)	14.43	13.56	7.88	7.36	3.54
FRR (%)	15.55	13.23	6.81	7.55	3.48
AER (%)	14.99	13.40	7.35	7.46	3.51

- *Group-2*. Table 4 aims to compare the authentication performance when users play Email applications and social networking applications. It is found that SVM classifier still outperformed the other classifiers, and that the error rate under *S2* is smaller than that under *S3* (i.e., both rates are below 3.6%: 3.02% vs. 3.51%). The results validate that users' touch behavior could become more stable under some tasks, and that it is easier to model their touch actions when using Email applications (due to smaller behavioral deviation).

Long-term Authentication. Similar to (Meng et al., 2019b), we also sought to explore the authentication performance after two weeks. A total of 28 participants (8 females; 12 of them are from Group-1) were willing to participate in this task. In particular, they would come to our lab and complete 5 sessions. A further $30 gift card was awarded to all participants. Figure 6 and Figure 7 show the average behavioral deviation for two groups, respectively.

- *Group-1*. Figure 6 compares the touch behavioral deviation between *S1* and *S2*. It is seen that the average deviation under *S2* is still much smaller than that under *S1*. This means that users' touch actions are stable when they play Email applications, in which an authentication scheme based on Email application usage could provide robust authentication performance.

- *Group-2*. Figure 7 compares the touch behavioral deviation between *S2* and *S3*. As compared with Group-1, the

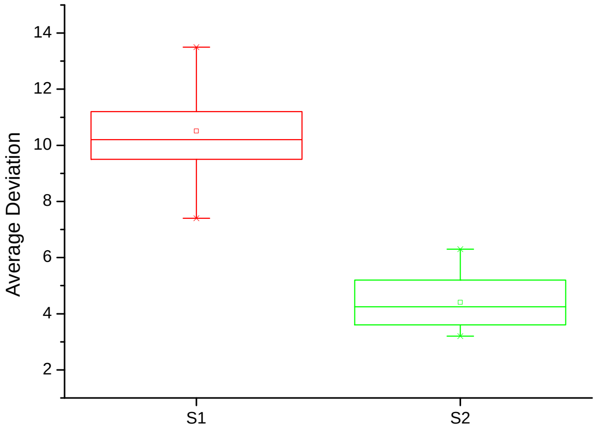

Fig. 6. The average behavioral deviation in Group-2 after two weeks.

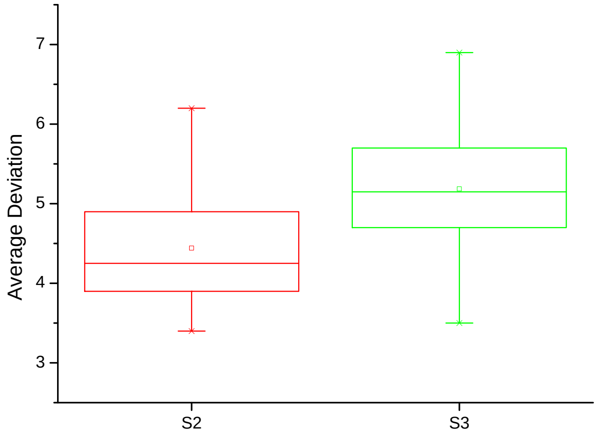

Fig. 7. The distribution of average deviation in Group-2 after two weeks.

gap is not significant, whereas the deviation under *S2* is still smaller than that under *S3*. After an informal interview with most participants, it is found that participants can have a clear behavioral pattern when they use Email applications, like checking and sending Emails. By contrast, their behavioral patterns may become more complicated when playing social networking applications, as these applications can provide many functions than Email applications.

Overall, though the deviation values in Figure 6 and Figure 7 are slightly higher than those in Figure 3 and Figure 5, users' touch actions on Email applications / social networking applications are much more stable than free task after two weeks. This implies that authentication schemes may provide more robust performance by verifying users when they play Email applications / social networking applications.

5. Discussion

Smart city is a promising architecture deployed with Information and Communication Technologies (ICT) and IoT devices (e.g., sensors, monitors), with the attempt to develop and deploy sustainable practices to address current challenges, i.e., handling rapid urbanization. Due to the complexity and increasing size of smart city, biometric authentication like behavior-based authentication can ease the movement among different facilities and enforce access control. Due to the wide adoption of smartphones under IoT context, Email applications are heavily used by most users. The design of a behavioral authentication scheme based on Email applications has a big potential to be acknowledged by populations, and the scheme itself would have good scalability.

Thus, this work focuses on touch behavioral authentication and explores users' touch behavior when they use smartphone Email applications. We also validate the observations reported by previous work, whereas there are still some challenges for future research.

Touch gesture types. This work mainly divides users' touch actions into single touch, touch movement and multi-touch, but does not consider specific actions such as zoom-in, zoom-out, rotate, etc. Generally, considering concrete touch gestures can benefit the authentication accuracy, but it depends heavily on users' touch habit. Due to the complexity, we plan to investigate the impact of concrete gestures in our future work.

Classifier selection. This work mainly studies five supervised classifiers including Decision tree, Naive Bayes, RBFN, BPNN and SVM. The authentication performance is comparable to the results reported by the existing literature. Typically, the authentication accuracy can be further improved by optimizing these classifiers. While how to optimize the parameters and settings of an algorithm is still a challenge.

Diverse algorithms. To explore the performance, this work mainly considers some traditional supervised classifiers, while other types of learning methods can be investigated like deep learning and transfer learning. Deep learning aims to mimic the structure and function of human brain to process data and detect objects. Transfer learning aims to train a model based on one task while being tested on another related task. This is helpful to enhance behavior-based authentication with data collected in different sessions.

Behavioral deviation. This work validates that users' touch behavior would become more stable (with smaller deviation) when they are given a task than free task. Even after some time, their behavioral deviation on using Email applications is greatly better than that on free task (and even social networking application usage). This implies a direction on designing appropriate authentication schemes based on given tasks.

Multimodal authentication. With the increasing complexity of IoT environments, there is always a need for multimodal authentication that combines several authentication mechanisms for better performance. For example, behavioral authentication can be enhanced by integrating with other biometrics such as physiological features (Fang et al., 2020), and ear and arm verification (Abate et al., 2019).

6. Conclusion

For IoT-enabled smart cities, smartphones would play an important role to facilitate people's daily lives, but these devices may also become the main target for cyber attacks. Hence there is an emerging need to design a proper authentication scheme to protect smartphones from unauthorized access. In this work, we focus on touch behavioral authentication that can provide a continuous verification, and explore the authentication performance when users interact with Email applications on smartphones. Our study with 60 participants demonstrated that users' touch behavior is more stable under Email application usage than free task, where an AER of around 2.9% (2.79% in Group-1 and 3.02% in Group-2) was achieved by using the SVM classifier. This implies that we can consider users' touch behavior under specific applications so as to design a more robust authentication scheme. Our work aims to stimulate more research in this area.

Acknowledgments

We would like to thank all participants for their hard work during the user study. This work was partially supported by National Natural Science Foundation of China (No. 61802077).

References

Abate, A.F., Nappi, M., Ricciardi, S., 2019. I-am: Implicitly authenticate me - person authentication on mobile devices through ear shape and arm gesture. IEEE Trans. Syst. Man Cybern. Syst. 49, 469–481.

Barra, S., Castiglione, A., Marsico, M.D., Nappi, M., Choo, K.R., 2018. Cloud-based biometrics (biometrics as a service) for smart cities, nations, and beyond. IEEE Cloud Comput. 5, 92–100.

Barra, S., Castiglione, A., Narducci, F., Marsico, M.D., Nappi, M., 2019. Biometric data on the edge for secure, smart and user tailored access to cloud services. Future Gener. Comput. Syst. 101, 534–541.

Buriro, A., Crispo, B., Gupta, S., Frari, F.D., 2018. DIALERAUTH: A motion-assisted touch-based smartphone user authentication scheme, in: Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy, Tempe, AZ, USA, March 19-21, 2018, ACM. pp. 267–276.

Cha, S., Kwag, S., Kim, H., Huh, J.H., 2017. Boosting the guessing attack performance on android lock patterns with smudge attacks, in: Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, Abu Dhabi, United Arab Emirates, April 2-6, 2017, ACM. pp. 313–326.

Chen, D., Ding, Z., Yan, C., Wang, M., 2020. A behavioral authentication method for mobile based on browsing behaviors. IEEE CAA J. Autom. Sinica 7, 1528–1541.

Dell'Amico, M., Filippone, M., 2015. Monte carlo strength evaluation: Fast and reliable password checking, in: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, October 12-16, 2015, ACM. pp. 158–169.

Deloitte, 2018. Global Mobile Consumer Survey. https://www2.deloitte.com/lu/en/pages/technology-media-and-telecommunications/articles/global-mobile-consumer-survey-luxembourg.html. [Online; accessed 25-May-2020].

eMarketer, 2017. Denmark has highest smartphone penetration rate in the world. http://www.netimperative.com/2017/12/06/denmark-highest-smartphone-penetration-rate-world/. [Online; accessed 25-May-2020].

Fang, L., Yin, C., Zhou, L., Li, Y., Su, C., Xia, J., 2020. A physiological and behavioral feature authentication scheme for medical cloud based on fuzzy-rough core vector machine. Inf. Sci. 507, 143–160.

Frank, M., Biedert, R., Ma, E., Martinovic, I., Song, D., 2013. Touchalytics: On the applicability of touchscreen input as a behavioral biometric for continuous authentication. IEEE Trans. Information Forensics and Security 8, 136–148.

Gartner, 2019. Enterprise and Automotive IoT Endpoints in 2020. https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io. [Online; accessed 19-May-2020].

Gomez-Barrero, M., Galbally, J., 2020. Reversing the irreversible: A survey on inverse biometrics. Comput. Secur. 90, 101700.

Liang, Y., Samtani, S., Guo, B., Yu, Z., 2020. Behavioral biometrics for continuous authentication in the internet-of-things era: An artificial intelligence perspective. IEEE Internet Things J. 7, 9128–9143.

Marsico, M.D., Mecca, A., Barra, S., 2019. Walking in a smart city: Investigating the gait stabilization effect for biometric recognition via wearable sensors. Comput. Electr. Eng. 80.

Meng, W., Hao, L.W., Ramanujam, M.S., Krishnan, S.P.T., 2015a. Charging me and I know your secrets!: Towards juice filming attacks on smartphones, in: Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, CPSS 2015, Singapore, Republic of Singapore, April 14 - March 14, 2015, ACM. pp. 89–98.

Meng, W., Jiang, L., Choo, K.R., Wang, Y., Jiang, C., 2019a. Towards detection of juice filming charging attacks via supervised CPU usage analysis on smartphones. Comput. Electr. Eng. 78, 230–241.

Meng, W., Li, W., Jiang, L., Meng, L., 2016a. On multiple password interference of touch screen patterns and text passwords, in: Kaye, J., Druin, A., Lampe, C., Morris, D., Hourcade, J.P. (Eds.), Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, San Jose, CA, USA, May 7-12, 2016, ACM. pp. 4818–4822.

Meng, W., Li, W., Jiang, L., Zhou, J., 2019b. Socialauth: Designing touch behavioral smartphone user authentication based on social networking applications, in: ICT Systems Security and Privacy Protection - 34th IFIP TC 11 International Conference, SEC 2019, Lisbon, Portugal, June 25-27, 2019, Proceedings, Springer. pp. 180–193.

Meng, W., Li, W., Wong, D.S., Zhou, J., 2016b. TMGuard: A Touch Movement-Based Security Mechanism for Screen Unlock Patterns on Smartphones, in: Manulis, M., Sadeghi, A., Schneider, S. (Eds.), Applied Cryptography and Network Security - 14th International Conference, ACNS 2016, Guildford, UK, June 19-22, 2016. Proceedings, Springer. pp. 629–647.

Meng, W., Wang, Y., Wong, D.S., Wen, S., Xiang, Y., 2018. *TouchWB*: Touch behavioral user authentication based on web browsing on smartphones. J. Netw. Comput. Appl. 117, 1–9.

Meng, W., Wong, D.S., Furnell, S., Zhou, J., 2015b. Surveying the development of biometric user authentication on mobile phones. IEEE Commun. Surv. Tutorials 17, 1268–1293.

Meng, Y., Wong, D.S., Schlegel, R., Kwok, L., 2012. Touch gestures based biometric authentication scheme for touchscreen mobile phones, in: Kutylowski, M., Yung, M. (Eds.), Information Security and Cryptology - 8th International Conference, Inscrypt 2012, Beijing, China, November 28-30, 2012, Revised Selected Papers, Springer. pp. 331–350.

Ometov, A., Petrov, V., Bezzateev, S., Andreev, S., Koucheryavy, Y., Gerla, M., 2019. Challenges of multi-factor authentication for securing advanced iot applications. IEEE Netw. 33, 82–88.

Sae-Bae, N., Memon, N.D., Isbister, K., Ahmed, K., 2014. Multitouch gesture-based authentication. IEEE Trans. Information Forensics and Security 9, 568–582.

Schechter, S.E., Tian, Y., Herley, C., 2019. Stopguessing: Using guessed passwords to thwart online guessing, in: IEEE European Symposium on Security and Privacy, EuroS&P 2019, Stockholm, Sweden, June 17-19, 2019, IEEE. pp. 576–589.

Shen, C., Zhang, Y., Guan, X., Maxion, R.A., 2016. Performance analysis of touch-interaction behavior for active smartphone authentication. IEEE Trans. Information Forensics and Security 11, 498–513.

Shen, M., Tang, X., Zhu, L., Du, X., Guizani, M., 2019. Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities. IEEE Internet of Things Journal 6, 7702–7712.

Song, Y., Cai, Z., Zhang, Z., 2017. Multi-touch authentication using hand geometry and behavioral information, in: 2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017, IEEE Computer Society. pp. 357–372.

Sundararajan, A., Sarwat, A.I., Pons, A., 2019. A survey on modality characteristics, performance evaluation metrics, and security for traditional and wearable biometric systems. ACM Comput. Surv. 52, 39:1–39:36.

Teh, P.S., Zhang, N., Teoh, A.B.J., Chen, K., 2016. A survey on touch dynamics authentication in mobile devices. Comput. Secur. 59, 210–235.

Wu, C., He, K., Chen, J., Zhao, Z., Du, R., 2020. Liveness is not enough: Enhancing fingerprint authentication with behavioral biometrics to defeat puppet attacks, in: 29th USENIX Security Symposium, USENIX Security 2020, August 12-14, 2020, USENIX Association. pp. 2219–2236.