THP: A Novel Authentication Scheme to Prevent Multiple Attacks in SDN-based IoT Network

Liming Fang, Yang Li, Xinyu Yun, Zhenyu Wen, Shouling Ji*, Weizhi Meng, Zehong Cao and M.Tanveer

***Abstract*—SDN has provided significant convenience for network providers and operators in cloud computing. Such great advantage is extending to the IoT network. However, it also increases the risk if the security of a SDN network is compromised. For example, if the network operator's permission is illegally obtained by a hacker, he/she can control the entry of the SDN network. Therefore, an effective authentication scheme is needed to fit various application scenarios with high-security requirements. In this paper, we design, implement and evaluate a new authentication scheme called The Hidden Pattern (THP), which combines graphics password and digital challenge value to prevent *multiple* types of authentication attacks at the same time. We examined THP in the perspectives of both security and usability, with a total number of 694 participants in 63 days. Our evaluation shows that THP can provide better performance than the existing schemes in terms of security and usability.**

***Index Terms*—Internet of Things, Shoulder-surfing, Password, Security and Privacy.**

I. Introduction

With the rapid development, SDN has received more and more attention. The central control of the SDN logic fundamentally improves the efficiency of the Internet, e.g., Internet of things (IoT), and promotes people to meet the needs of various applications in innovative network ways. In the IoT environment, SDN can provide flexible, dynamic and automatic network reconfiguration by using centralized control and abstract network devices. The typical structure of an SDN network is shown in Figure 1. Given the complexity and scale of the IoT network, it is infeasible to manage the network manually. Thus, SDN provides a viable, cost-effective way to manage the IoT network by ensuring the network and data security, reducing bandwidth consumption and maximizing application performance.

However, once the SDN controller is compromised, attackers can quickly affect the whole network and cause great harm. Therefore, there is a need for developing a strong authentication scheme for the SDN controller to reduce the risk of SDN controller being attacked. In the IoT environment, administrators can use mobile devices or IoT devices to check the network situation and control the network, when they are working on the field. In such scenario, there should be a secure login authentication scheme for mobile devices or IoT devices. With the emergence of various advanced attacks on login authentication systems, it is hard for simple login authentication methods/traditional passwords to protect users' private information. Even the biometric authentications such as fingerprints and facial recognition could be easily cracked [1]. As a result, there have been tremendous efforts in developing new authentication methods to prevent different attacks [2]–[5].

Currently, text-based password and graphic-based password are widely used for login authentication. However, most simple text passwords can be cracked through Random guessing attack [6] or Dictionary attack [7] with the increasing computing power. While if we set up a kind of complex text-based password, it may increase the burden of memory as well as the frequency of resetting their passwords [8]. The graphic-based password can be easier to remember and more suitable for long-term memory, compared to textual password according to previous studies like [9]–[12]. However, graphics-based password schemes are vulnerable to shoulder-surfing attacks [13] [14], and most of the schemes are not designed for IoT devices with small screens. For smartphones, the smudge attack breaks the authentication by analyzing the screen trace. Therefore, it can be used to attack both types of password, but it may fail when the password is complex enough, making the trace unanalyzable [15] [16]. Recording screen attack captures all information from the screen, which can creak any type of passwords [17] [18] mentioned above.

Motivated by this challenge, in this work, we propose a new graphical authentication scheme, which can prevent a variety of attacks, while ensuring the usability (i.e., users do no require to remember a complicated password and there is no need for extra devices for their authentication). Our solution consists of two phases: registration phase and the authentication phase. In the first phase, users should choose the pattern including his login password (a graph) and the image area. In the authentication phase, the user will obtain a 2-digit challenge value through the pattern. The authentication can be obtained if and only if the challenge value is correctly matched with the image area. This method prevents many types of attacks

* Shouling Ji is the corresponding author.

Liming Fang, Yang Li and Xinyu Yun are with College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, NO.29 Yudao Street, Nanjing, China. E-mail: {fangliming, lyang0314, yunxinyu}@nuaa.edu.cn.

Zhenyu Wen is with Newcastle University. E-mail: Zhenyu.wen@newcastle.ac.uk

Shouling Ji is with the Institute of Cyberspace Research and College of Computer Science and Technology, Zhejiang University, Hangzhou, Zhejiang 310027, China, the Alibaba-Zhejiang University Joint Institute of Frontier Technologies (A.Z.F.T.), Hangzhou, China, and with the School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, Georgia 30332, USA. E-mail: sji@zju.edu.cn

Weizhi Meng is with DTU Compute, Technical University of Denmark, Denmark. E-mail: weme@dtu.dk

Zehong Cao is with University of Tasmania. E-mail: Zehong.Cao@utas.edu.au

Tanveer M. is with Indian Institute of Technology Indore. E-mail: mtanveer@iiti.ac.in

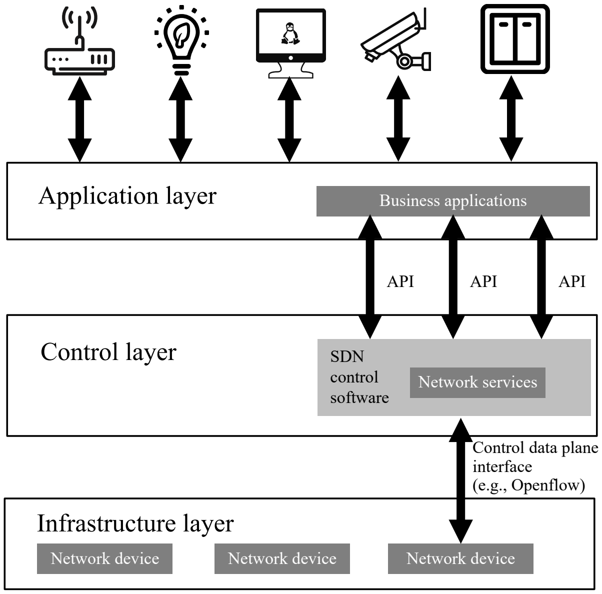


Fig. 1: The structure of SDN network.

including shoulder-surfing, smudge and recording screen, since the system passes the challenge value implicitly and randomly.

Further, we conduct three experiments i.e., security experiment, usability experiment, and chronicity experiment to evaluate the performance of our proposed scheme. To facilitate the experimental investigation and collect the experimental data, our THP was developed and deployed on the mobile phones. In the study, we involved a total of 694 participants for 63 days. Our evaluation results demonstrate that THP can efficiently prevent multiple attacks like shoulder-surfing, smudge and recording screen attacks, while ensuring usability and chronicity.

A. Contributions

Our major contributions of this paper can be summarized as follows:

- We design and implement a new security login authentication scheme based on both the graphical password and text-challenge value. It resists a variety of attacks, such as shoulder-surfing attacks, smudge attacks, and recording screen attacks. In addition, our scheme does not require any additional device (see the detail in §III).
- We add an advanced policy into our scheme to increase the flexibility. Users can decide the number of "patterns" in their scheme to fit their scenarios, according to different security requirements (see the detail in §III-B).
- In the security experiment, we reproduce 1475 attack trials, including 1320 trials of shoulder-surfing attack, 100 trials of smudge attack and 55 trials of recording screen attack. Our method can fully defend against the shoulder-surfing and smudge attacks in every case. For the recording screen attack, our scheme can fully defeat against it in normal case while having the possibility to fail in an extreme case (see the detail in §IV).
- The usability experiment evaluates the login time of our scheme. Basically, the average login time of the proposed scheme is 20.9094 seconds, and the skilled user only needs 6 seconds (see the detail in §V). Compared with other existing schemes that can only resist one or two attacks, our scheme has similar usability performance, for example, the average login time of MobSecure is 18.1 seconds [19], and the average login time of BWPIN is 16.50 seconds [5].
- We also design a chronicity experiment considering the case that users have not used their password for a long period of time. Our evaluation shows that up to 99.14% of users can still remember their username and password after 20 days with our scheme (see the detail in §VI).

This paper is structured as follows: §II introduces the relevant background and attack models. Our THP scheme is detailed in §III. In §IV, we evaluate the security of our scheme with different emulated attacks in real testbeds. In §V, we evaluate the usability of our THP, and the chronicity experiments are described in §VI. Finally, we compare THP with other schemes and conclude the work in §VII.

II. Related Work

In this section, we explicate the attack models that are considered in this work and then compare our THP with other related work.

A. Attack Models

a) Shoulder-surfing Attack: In the process of login authentication, the process of operating the screen is easy to be peeped. For example, attackers can capture users' login authentication information through video recording or direct observation. The shoulder-surfing attack can be divided into single shoulder-surfing attack and multiple shoulder-surfing attack. The single shoulder-surfing attack means that an attacker only has one chance to see the credentials. However, the attacker can capture the credential many times under a multiple shoulder-surfing attack. The later usually requires some devices like a camera to replay the scenario of the information leakage. Thus, the attacker can have sufficient time to analyze the captured information to break the scheme.

Moreover, we are surrounded by CCTVs which can cause many security risks, i.e., it can be easily controlled by the attacker for compromising other high-security systems through multiple shoulder-surfing attack. We investigated the cameras, commonly used within a 5 km radius of our lab, and then evaluated the security of several cameras that we obtained. The table I shows that some cameras commonly used in public places have certain security problems which open opportunities for attackers to perform shoulder-surfing attack. The parameters in the table I are explained as follows:

- Definition. Definition refers to the resolution of the cameras. Attackers who use cameras for shoulder-surfing attacks usually choose high-resolution cameras such as 720P, 960P and 1080P.
- Focal length. The focal length of an optical system is used to measure the intensity of the system converges

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2944301, IEEE Internet of Things Journal

TABLE I: Details of the cameras with high frequency use.

	JA-Q3*	YSY-BJXQ	IPY-66	HIKVISION C6	Z-BEN WK-304	Haier WSC-580W	Xm 870
Definition	960P	960P	1080P	720P	720P	960P	1080P
Focal length	2.8mm	4mm	2.8mm	4mm	2.8mm	3.6mm	2.8mm
Built-in WebShell utilization	17.5%	21.4%	10.9%	21.2%	14.7%	32.1%	28.8%
Weak password	√	√	√	√	√	√	√
Bypass the authentication	√	×	×	√	×	√	√
Protocol vulnerability	×	×	√	×	√	×	√

or diverges light. It can affect the clarity of information acquired by an attacker through shoulder-surfing attacks.

- Built-in WebShell utilization. Each camera can be controlled from the built-in webshell, and the built-in webshell can capture the content recorded by the camera. If the built-in webshell utilization is low, it means the authentication password is most likely the initial password, which increases the risk of privacy being leaked.
- Weak password. Weak passwords are easy-to-decipher passwords, including simple numeric combinations, numeric combinations with the same account number, adjacent keys on the keyboard, or common names (such as "123456", "$abc123$", "$Michael$", etc). The general passwords of the terminal device factory configuration are all in the category of weak passwords. Weak passwords an attack can easily control the camera.
- Bypass the authentication. Bypass the authentication is whether the administrator or user can operate the camera without authentication. If the attacker can bypass the authentication process, the control of the camera is able to be obtained easily.
- Protocol vulnerability. The communication protocols that are used on various cameras may present vulnerabilities during configuration and connection. They may provide the opportunities for the attackers to obtain the control of the cameras.

b) Recording Screen Attack: Recording screen attack is a very powerful attack and very hard to prevent. The attacker uses the vulnerability of the IoT devices to install illegal applications to record all the information displayed on the screen [17] [18]. According to our survey, Android operating system allow programmers to write code that contains the meaning of forbidding screen recording when developing applications. However, iOS operating system does not have this operation [20]. It only reminds the user that some malware are recording the screen operations, and does not forbid the malware the activity. The recorded screen content stores in the user's mobile phone album, and the attacker can get the complete video by accessing system album illegally. Such attack can easily obtain the login authentication credentials. To the best of our knowledge, most current authentication schemes are not resistant to the recording screen attack.

c) Smudge Attack: Smudge attack is based on the traces such as fingerprint that user has left during his/her operation on the devices [21]. According to the current use of mobile devices or electronic touch screens, it is very easy for users to leave their traces on the screen. For some login authentication schemes that leave a fixed trace on the screen, such as the screen unlock scheme connected by the gesture, it is very easy to be cracked by smudge attacks.

B. Authentication Schemes

a) Graphic-based Login Authentication Scheme: Yu et al. proposed a new graphic-based authentication scheme named EvoPass [23]. In this scheme, the certified image is processed into grayscale image and decoy image by an image processing algorithm, as to reduce the identification information contained in each certified sketch and evolve the certified sketch into more versions resistant to shouldersurfing Attacks. EvoPass gradually increases password strength by reducing the amount of information contained in authentication sketches.

Claude et al. proposed a similar concept that process the Mooney images by using special algorithms [24]. The user then utilizes implicit memory to identify the processed images. This authentication scheme provides a novel idea for the graphic-based login authentication scheme, but there are still some similarities between the processed images and the original images.

These schemes can still be easily cracked by those attacks that can capture high-definition login procedures such as recording screen attacks.

b) Image and Text Combined Authentication Scheme: In 2016, Chakraborty et al. proposed a scheme of MobSecure [19], which designs a special interactive interface consisting of 36 password points, each of which represents a number or letter, and has a variety of colors. When a user tries to log in, he is required to click the password point 4 times to complete the unlock. The password point clicked by the user is not the real password, it is generated by the user's password and the challenge value transmitted by the system. Therefore, this scheme can effectively prevent shoulder-surfing attackers from otaining the real password. However, the transmission of the challenge value relies on external tools, such as headphones. As a result, the application scenarios of this scheme are greatly limited, and it lacks convenience.

Nyang et al. proposed TTU in [25] that resists shoulder-surfing attack from the perspective of the human body structure and physics. It requires the user to obtain the challenge value and puts his thumbs on a fixed position of the screen. Then, the system can be unlocked when the challenge value being shown on the screen. When the user makes a specific gesture according to the requirement, the palm will block the key information on the screen so as to achieve the purpose of resisting shoulder-surfing attack. Although this method is logically feasible and the security of the scheme has been tested in practice, it still has the disadvantage of poor convenience. Because when

TABLE II: Comparison of different schemes

Scheme	Shoulder-surfing Attack	Smudge Attack	Recording Screen Attack	Convenience
PassPoints [22]	×	×	×	×
EvoPass [23]	√	√	×	×
Mooney [24]	√	√	×	×
MobSecure [19]	√	√	×	×
TTU [25]	√	√	×	×
PassMatrix [26]	√	√	×	×
PIN [27]	×	√	×	√
FakePointer [28]	√	√	×	×
Color Rings [29]	√	×	×	×
Convex Hull [30]	√	√	×	×
S3pas [31]	×	√	×	×
Z.Zheng's Scheme [32]	×	×	×	×
L.Wang's Scheme [33]	×	×	×	×
V.Roth's Scheme [34]	√	√	×	×
S.wiedenbeck's Scheme [35]	√	√	×	×
Color Pass [36]	√	√	×	×
Tinylock [15]	×	√	×	×
Zezschwitz E V's Scheme [37]	×	√	×	×
Kwon T's Scheme [14]	√	√	×	×
Yan Q's Scheme [38]	√	√	×	×
Zakaria NH's Scheme [39]	√	√	×	×
Our Scheme THP	√	√	√	√

using this scheme for login authentication, both hands must be placed on the screen at the same time to make a fixed gesture, which is inconvenient for users who are accustomed to using only one-handed to operate devices.

PassMatrix scheme proposed by Sun et al. also has the convenience problem [26] . Although it is effective for resisting shoulder-surfing attack, the transmission process of challenge value requires the user to make fixed gestures on the screen, which is not convenient for users. Moreover, the scheme cannot resist recording screen attack, because the challenge value can be captured from the screen when the special action is performed.

c) Biometric-based Login Authentication Scheme: In addition to visual-based login authentication schemes, such as graphic-based passwords and textual passwords, many devices tend to use humans' physical characteristics during the authentication process, which is convenient and quick. For instance, fingerprint recognition and face recognition are based on these advantages. However, with the advancement of technology, fingerprints can be easily counterfeited [40], and face recognition has recently been cracked by 3D printing technology [41], so the best way to solve these problems is to be able to effectively detect the liveness of the face. However, it is very difficult in practice. At the Black Hat 2019, Tencent invented a pair of glasses that can crack the face recognition by destroying the liveness detection in face recognition [42]. People need some new and innovative solutions that are different from the past.

In comparison, our THP does not require the user to involve an additional audio transmission device or make fixed gestures during authentication. More importantly, the system challenge value is hidden in every pattern randomly appearing in the transmission process. The whole process is implicit. Even if an attacker records the whole process of authentication, he or she still cannot determine which pattern is selected by the user. To the best of our knowledge, our scheme is the first one that can defend against all three attacks (shoulder-surfing attacks, smudge attacks, and recording screen attacks) at the same time. Table II compared our method with serval recent papers.

Algorithm 1 Registration

```
Require:
    $N$, the User Name input at registration by the user
    $P$, the pattern selected at registration by the user
    $I$, the image selected at registration by the user
    $Sq$, the square selected at registration by the user in the image
Ensure:
    Result of Registration
if $N$ is not existed in the database then
    The server stores $\{N, P, I, Sq\}$ in the user database.
    return true.
else
    return false.
end if
```

III. Our Scheme: THP

In this section, we first describe the design and the operation workflow of THP, and then present an advanced strategy which dynamically adjusts the security levels of our scheme to adapt it to different scenarios to meet the various security requirements.

A. THP Implementation

In order to simultaneously deal with shoulder-surfing attack, smudge attack, and recording screen attack while ensuring usability, we our authentication scheme is based on graphical password. The construction of the THP is shown in figure 2. Our THP consists of *registration phase* and *authentication phase*. The modules (labeled by purple) represent the actions performed by the system, and the actions performed by user

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2944301, IEEE Internet of Things Journal

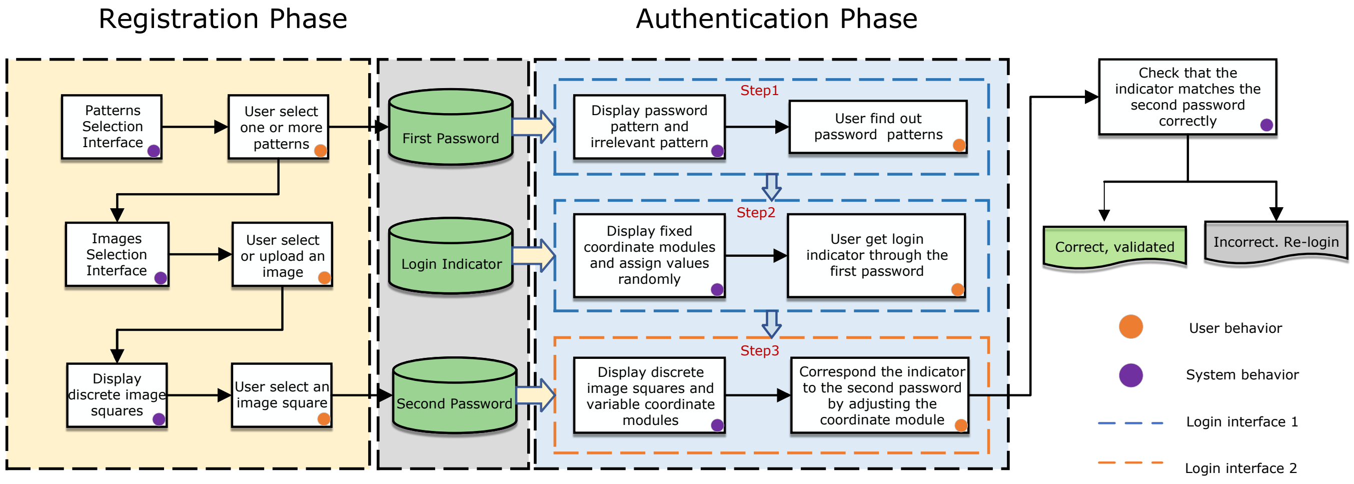

Registration Phase
Authentication Phase
Patterns Selection Interface
User select one or more patterns
Images Selection Interface
User select or upload an image
Display discrete image squares
User select an image square
First Password
Login Indicator
Second Password
Step1
Display password pattern and irrelevant pattern
User find out password patterns
Step2
Display fixed coordinate modules and assign values randomly
User get login indicator through the first password
Step3
Display discrete image squares and variable coordinate modules
Correspond the indicator to the second password by adjusting the coordinate module
Check that the indicator matches the second password correctly
Correct, validated
Incorrect. Re-login
User behavior
System behavior
Login interface 1
Login interface 2

Fig. 2: The construction of THP

are labeled by orange. Figure 4a and 4b are the screenshot of the login interface 1 (see the blue dotted line box in figure 2) and the login interface 2 (see the orange dotted line box in figure 2).

To have a better understanding of THP design, we illustrate the construction of our THP through an operation (or execution) workflow in the following, which is summarized in Algorithm 1 and 2. Firstly, a new user should do the registration (the workflow is illustrated in figure 2 with orange label). In this phase, the user is asked to provide 2 passwords: *first password* and *second password*. To select the *first password*, the user is asked to choose 1 pattern via the pattern selection interface as shown in figure 3a. The screenshot (see figure 3a) illustrates that the "panda" is selected as the *first password* and user must remember his *first password* for authentication phase.

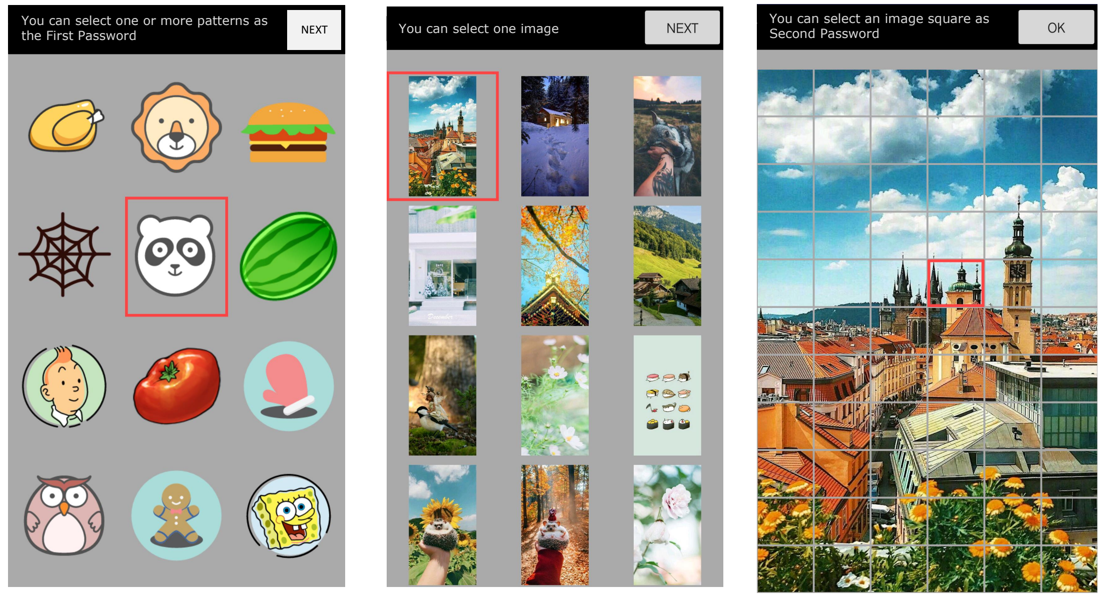
Next, the user is required to select or upload an image as shown in Figure 3b through picture selection interface (see registration phase in Figure 2) at the phase of registration. The selected or uploaded image is divided to 6*11 squares; the user is required to choose one as the *second password* (see the red square in Figure 3c). Obviously, this password should be memorized. Then the user finishes the registration phase.

Algorithm 2 Authentication phase

```
Require:
    $UN$, the user name input at authentication by the user
    $USq$, the square corresponding to the login indicator
    $LN$, the number of the user login
    $N$, the user name stored in the database
    $Sq$, the square in the image stored in the database
Ensure:
    Result of Login
if $UN$ is the same as $N$ then
    The server generates a login indicator.
    Set $LN = 1$.
    repeat
        if $USq$ is the same as $Sq$ then
            return true.
        else
            if $LN$ is more than 5 times then
                return false.
            else
                $LN = LN + 1$.
            end if
        end if
    until $USq$ is the same as $Sq$ and $LN$ is less than 5 times
else
    return false.
end if
```

In the authentication (login) phase, summarized in the Algorithm 2, the system first generates a *login indicator* for a user, which is a coordinate value, corresponding to the *first password*. We designed a method to pass the *login indicator* implicitly. For example, Figure 4a illustrates that 66 patterns are generated and only 1 pattern is the selected *first password* (e.g., only 1 "panda" existing). Other 65 patterns are generated randomly from the pattern database (we stored 132 non-repeat pictures as the patterns in the pattern database), therefore, the duplicate patterns may contain. The *login indicator* can be different in each login process, because all the 65 patterns and the order of the 2 coordinates are randomly generated. This process is illustrated in the *step 1* during the authentication phase. Moreover, the coordinate (see the top and leftmost in 4a) is used to assign the value to each pattern. Hence, the user needs to identify his/her *first password* and its coordinate value. In this example, the coordinate value of "panda" is $(8, F)$ (*Step 2* in authentication phase illustrates the process). Since the position of *first password* and the order of coordinates are changed in each login process, they can change the *login indicator* randomly. Moreover, in *step1* and *step 2*, the user is not required to do any actions. Thus, the attacker cannot obtain the *first password* or *login indicator* via any above mentioned attacks.

Once the *login indicator* is generated, the user just needs



You can select one or more patterns as the First Password

You can select one image

You can select an image square as Second Password

(a) Select a ”panda” from the many patterns when the user registering.

(b) Select a picture from the picture database.

(c) Choose one of the many squares separated by a picture as the password point.

Fig. 3: The registration phase.

to remember the coordinate value corresponding to his/her *first password* for current login process, and use it to match with his/her *second password* to unlock the system. After the user notices the system by clicking “NEXT” in Figure 4a, a new interface (see Figure 4b) is displayed on the screen triggered by (step 3 in authentication phase). In this interface, we designed a swappable coordinate. The top coordinate can be swapped left and right and the left coordinate can be swapped up and down. Users can use their fingers to swipe the left coordinate up and down and top coordinate left and right. However, the divided background image is not moving while we swapping the coordinates. The range of the left coordinate is from 1 to 11 and the top coordinate is from A to F. Thus, the small square (*second password*) selected by user in Figure 3c has a corresponding coordinate value $(5, A)$ in Figure 4b. If the user swipes 6 units up on left coordinate and 2 units left on top coordinate, the coordinate value for the selected small square is $(8, F)$ as shown in Figure 4c. In this case, coordinate value of *second password* can match the coordinate value of *first password*, then the authentication is successful.

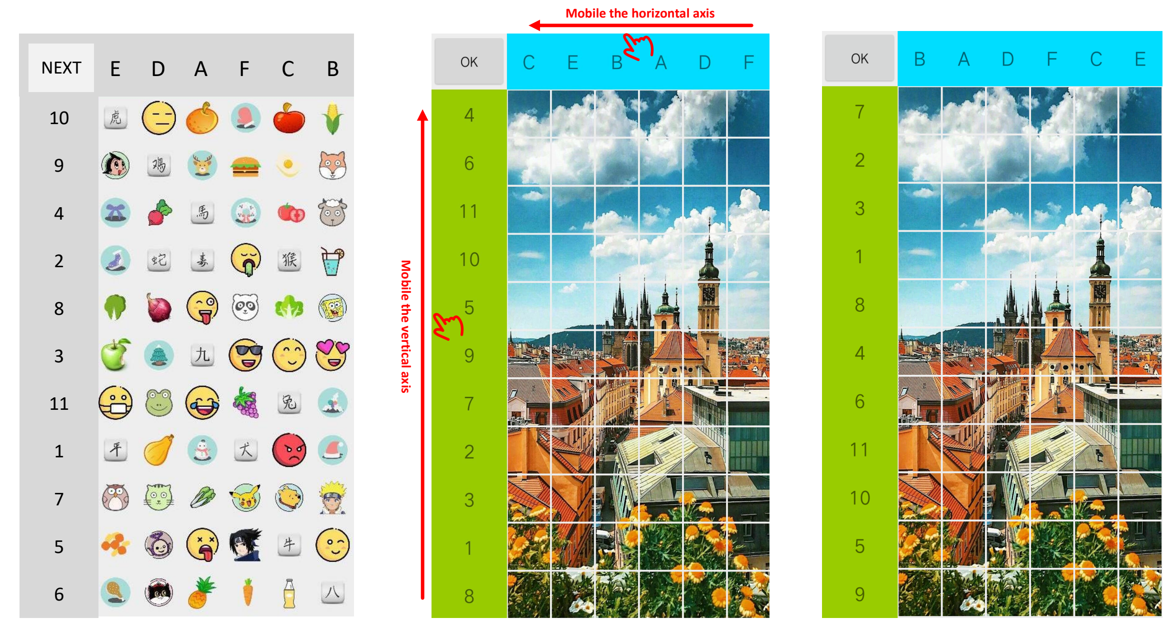
When the user is swiping the coordinates, the coordinate value corresponding to each square in the image keeps changing. The attacker has no idea about the *first password*, *second password* and *login indicator*.

a) Weakness: Our THP can offer better performance than other schemes to prevent the above-mentioned three attacks. However, it is not impossible to be cracked. For example, if a attacker can obtain at least 2 different login process videos completely via the recording screen attack. Then, by comparing the 2 videos, the attacker may have the chance to find the common patterns which appear only once in both videos. Then, the attacker can record the corresponding *login indicators* of each obtained patterns. Based on these *login indicators*, the attack has to traverse all small squares (660 in total, see Figure 4b) for each *login indicator*. Although the process is cumbersome, it provides the possibility for an attacker to crack our scheme.

B. Advanced Strategy

To further improve the security of our scheme, we designed an advanced strategy that allows users to dynamically adjust the login scheme according to their security requirements. In the registration phase, users can decide the number of *first passwords*. When users select patterns (*first passwords*), they can choose multiple patterns at the same time, and then remember all selected patterns accurately. The patterns' selection order will not influence of the login process. Because, in authentication phase, the system randomly selects one of the selected patterns for users to do the login, referred to step 1 and 2 in Figure 2. Due to the appearance of *first password* is random, the user doesn't need to care about the order of the selection during the registration phase. For the remaining 65 patterns on the screen, the system randomly selects the remaining non-user password patterns. With this method, even if the attacker obtains 2 complete login process videos, users may not use the same pattern as the *first passwords*. Therefore, the attacker needs to obtain more videos of recording the login process.

In addition, it is vulnerable to hot-spot guessing attack when using graphic-based login authentication schemes. For example, comparing some colorful and single-color patterns, people tend to choose some special patterns as their own passwords, which is easy to remember. This issue appears in most graphic-based login authentication schemes like [26] [43] [44] [45]. In order to avoid this problem, in our THP system, we allow the users to upload their own pictures. Then, we set



(a) The interface of passing the login indicator.

(b) Enter the initial status of login password.

(c) Complete the password.

Fig. 4: The authentication phase.

the pattern display mode in registration process to random. All these aim to reduce the security risk brought by “selection trend”.

IV. Security Experiment

In this section, we evaluate the performance of our THP in the aspect of resisting multiple attacks in the real testbeds.

A. Experimental Setup

a) Experimental Setting: We implemented THP login system on both Android and iOS platforms. In particular, 132 patterns were designed in the pattern database, and 40 preset pictures were provided in the picture database as the background. Also, we provide an option for users to upload their pictures(referring to Figure 3c). This can help users easily memorize their *second password* with a familiar picture. For ordinary users, the registration process is performed in a secure environment, without any malicious attacks, and ensuring the communication security between the client and the server. For shoulder-surfing attack and smudge attack, we require the users to create only one pattern as the *first password*. Notably, for the screen recording attacks, the participants were asked to create different numbers of patterns as their *first password*, including 1, 2 and 3 patterns.

b) Participants: We randomly selected 300 people from the 694 participants. The experiments lasted for 32 days and we used the most popular mobile phone models as shown in Table VI.

c) Experiment Instruction: We distributed the user manual of THP to each participant and make sure they understand the process of THP. Before the experiment, participants could perform some appropriate practices. We randomly split participants into two group: attackers and ordinary users. Then, we explained the behaviors of each group to ensure that they understand their roles in the experiments.

d) Experimental Results Recording: We defined the maximum attack time is 24 hours, and record the successful cracking in every hour. If a participant cracks within an hour, we still record the successful cracking time as 1 hour. The successful cracking must meet the following requirement: *the attacker needs to obtain the user’s all password patterns, including the multiple patterns selected for the* first password.

e) Experimental Investigation: After the completion of each round of experiment, the attackers were given a questionnaire as shown in table IX which allows us to investigate the reasons of success attacks and the failures.

B. Implementation

a) Shoulder-surfing Attack: We consider two types of shoulder-surfing attack: naked eye attack and camera attack. The camera model is EZVIZ cs-c6-21wfr-b. In the experiment, we selected 300 participants and divided them into 30 groups. Each group has 10 participants, including 2 attackers and 8 ordinary users. One attacker conducted a naked eye attack and another used the camera for attacking. Each ordinary user was attacked three times, so each group has 48 attacks and the whole experiment has 1440 attacks in total.

Figure 5 shows the shoulder-surfing attack by using the camera. The camera is about 1.1 meters away from the participant who acts the ordinary user. The attacker who performs the naked eye attacks is about 1 meter away from the ordinary user. The attacker observed the authentication process only once from entering the username until the successful login. Attackers were allowed to record critical information to help them remember the login process. The time spent for each attack was recorded for further evaluation.

TABLE III: Results of Security Experiment

Attack Types	Shoulder-surfing Attack		Recording Screen Attack				Smudge Attack
Details	Naked Attack	Camera Attack	1	2	3	5	
Total number of effective attacks	624	624	5	10	15	25	100
Number of successful cracking in an hour	0	0	0	0	0	0	0
Crack successfully rate in an hour	0%	0%	0%	0%	0%	0%	0 %
Number of successful cracking in two hours	0	0	0	0	0	0	0
Crack successfully rate in two hours	0%	0%	0%	0%	0%	0%	0 %
Number of successful cracking in five hours	0	0	0	0	1	1	0
Crack successfully rate in five hours	0%	0%	0%	0%	20%	20%	0 %
Number of successful cracking in twelve hours	0	0	0	1	2	2	0
Crack successfully rate in twelve hours	0%	0%	0%	20%	40%	40%	0 %
Number of successful cracking in a day	0	0	0	2	2	3	0
Crack successfully rate in a day	0%	0%	0%	40%	40%	60%	0 %

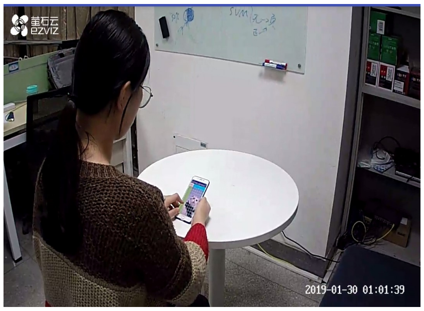


Fig. 5: The experiment about shoulder-surfing attacks.

TABLE IV: Smudge distance

	U_1	U_2	U_3	U_4	U_5
Horizontal-a	4.23cm	1.15cm	2.64cm	3.33cm	4.59cm
Horizontal-b	3.31cm	2.97cm	3.65cm	1.54cm	4.42cm
Horizontal-c	5.14cm	4.43cm	1.15cm	0.98cm	3.18cm
Horizontal-d	1.76cm	5.09cm	3.29cm	1.94cm	4.72cm
Horizontal-e	2.33cm	0.97cm	4.05cm	4.56cm	0.89cm
Vertical-a	2.91cm	5.65cm	3.78cm	9.44cm	5.27cm
Vertical-b	6.34cm	8.29cm	8.2cm	6.38cm	0.88cm
Vertical-c	4.23cm	7.3cm	3.44cm	7.31cm	4.04cm
Vertical-d	1.92cm	4.86cm	0.96cm	6.39cm	5.29cm
Vertical-e	2.54cm	6.48cm	2.67cm	7.46cm	9.17cm

b) Smudge Attack: For this attack, intruders cannot observe the login process, but can obtain the fingerprints from the screen. We consider a successful attack as: the attacker is able to log into the system by analyzing the user's fingerprints left on the screen.

We randomly selected 20 participants from 300 participants and divided them into 10 groups. Each group has one attacker and one ordinary user. We recorded the time consumption that the attacker needs to crack the authentication. At the end of each login process, the attacker got the mobile phone and guessed the users password through trace information. This experiment produced 100 attacks.

Table IV shows the trace information left on the screen after 5 participants performed the login operations. For example, as shown in Figure 4b and 4c, if the user moves "8" to the original position of "5", then this distance is the vertical axis movement distance. Similarly, if the user moves "F" to the original position of "A", this distance is the horizontal axis movement distance. The user's fingers could left the traces on the screen as they move the horizontal and vertical axes.

c) Recording Screen Attack: The attacker implanted the recording screen software inside the mobile phone under the ignorant of ordinary users. We emulated the action of malicious software that recorded the login process of users through the screen recording function of the phone and provided it to the participants who acted as attackers. Similarly, we recorded the time consumption that a attacker needs to perform a successful attack.

This experiment randomly selected 40 participants from 300 participants and divided them into 20 groups, with 2 participants in each group. 1 play attacker and the other 1 play ordinary user. In reality, malware may attack many times for a long period of time, so we recorded the results and time of different attacks. The frequencies of performing the screen record are 1, 2, 3 and 5 respectively, and each one has 5 groups. In addition, we also asked the participants from 20 groups to use 1, 2 and 3 patterns as their *first password* in the experiment and the pattern should not be repeated for each experiment. The total number of attacks was 165.

C. Experimental Results and Analysis

In this subsection, we analyze the experimental results, which are summarized in Table III.

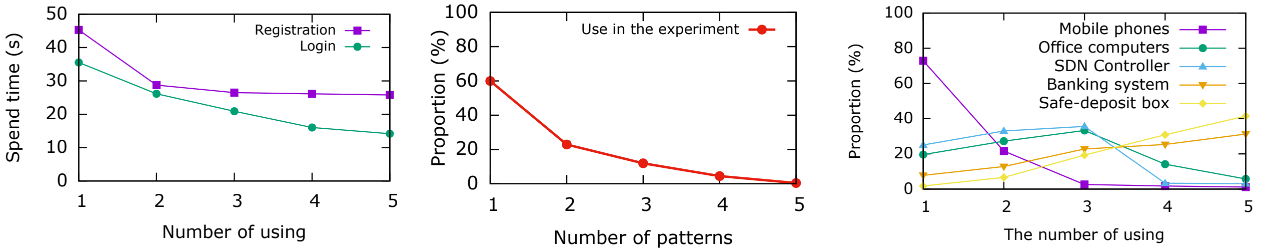
It is worth noting that 300 participants involved in the shoulder-surfing attack experiment; 260 participants completed the authentication process. There are a total of 1248 attacks, including 624 naked eye attacks and 624 camera attacks. The results in Table III indicate that no attack can crack our authentication scheme. We interviewed the attackers after the experiments, the reasons that cause the failure of the shoulder-surfing attack can be summarized as follows:

- User's login time is too short, so that the attacker cannot effectively capture the login information.
- The camera could not clearly capture login information.
- Although the attacker can observe the login process, he/she cannot obtain sufficient information to break our system.

a) Smudge Attack: All the participants completed the experiment and no attack can successfully crack our system. The feedbacks from the attackers illustrate that the traces left on the screen are very different for each login process. This

TABLE V: Results of Recording Screen Attack

Number of patterns	1				2				3			
Number of screen recording	1	2	3	5	1	2	3	5	1	2	3	5
Total number of effective attacks	5	10	15	25	5	10	15	25	5	10	15	25
Number of successful cracking in 1 hour	0	0	0	0	0	0	0	0	0	0	0	0
Crack successfully rate in 1 hour	0%	0%	0%	0%	0%	0%	0 %	0%	0%	0%	0%	0 %
Number of successful cracking in 2 hours	0	0	0	0	0	0	0	0	0	0	0	0
Crack successfully rate in 2 hours	0%	0%	0%	0%	0%	0%	0 %	0%	0%	0%	0%	0 %
Number of successful cracking in 5 hours	0	0	1	1	0	0	0	0	0	0	0	0
Crack successfully rate in 5 hours	0%	0%	20%	20%	0%	0%	0 %	0%	0%	0%	0%	0 %
Number of successful cracking in 12 hours	0	1	2	2	0	0	0	0	0	0	0	0
Crack successfully rate in 12 hours	0%	20%	40%	40%	0%	0%	0 %	0%	0%	0%	0%	0 %
Number of successful cracking 24 hours	0	2	2	3	0	0	0	1	0	0	0	0
Crack successfully rate in 24 hours	0%	40%	40%	60%	0%	0%	0 %	20%	0%	0%	0%	0 %



(a) Change of registration and login time.

(b) Percentage of patterns selected by users.

(c) A survey of the number of patterns selected by users in different scenarios.

Fig. 6: Investigation of users

is because the positions of the login indicator and the *"first password"* could change randomly every time when the user enters. As the user has to perform different operations on the screen each time, there are no fixed traces left. In this case, the smudge attack cannot obtain the useful information.

b) Recording Screen Attack: There are 40 participants performed the recording screen attack experiment, and all the participants completed their tasks. The number of screen records can affect the attack successful rate significantly. Specifically, we divided our experiment into 4 settings: 1 screen record, 2 screen records, 3 screen records and 5 screen records. The results as shown in Table III indicate that if the attacking time is set to 2 hours, there is not successful attack. With the increase number of screen record, the possibility of cracking our scheme incases. For instance, 60% attacks can crack our system when the attacking time is 24 hours with 5 screen records. In practice, there are limited screen recording resources as well as analyzing time available for the attacker. It is worth mentioning that the process of analyzing and cracking may cost a lot of time on the attackers' side. The time they spent is also shown on the table. We also detailed the statistics in in Table V that shows the cracking rate and the time of using different patterns as the *"first password"*. Other details of this experiment are shown in the Table VI, which contains detailed information of all participants in our safety experiment.

V. Usability Experiment

In the section, we evaluate the usability of our THP by measuring the following metrics: *a)* the time cost of login to the system for new user and the skilled user who has been practiced many times; *b)* users' security preferences in different scenarios; *c)* the number of patterns being selected by each participant; *d)* comparisons with biometric authentication scheme.

A. Experimental Setup

a) Experimental Setting: We used the same implementation of THP in the security experiment, and added some interfaces on the server side to allow us to easily obtain the experimental data, including the time cost of login and the login date & time for each user. The mobile phone models used in this experiment are listed in Figure 9 (see appendix).

b) Participants: The experiment recruited up to 694 participants who performed 677 time of experiments; and the entire experiment lasted for 63 days. The average age of participants was 33.6 years old, and their age, occupation and other specific information are summarized in Table VIII.

c) Experimental Investigation: We designed a user questionnaire and distributed it to each participant to collect users' feedbacks and their preferences.

B. Experimental Results and Analysis

In this subsection, we evaluate our authentication scheme in the following metrics: *a)* time cost of login and registration; *b)* users' preferences of the patterns; *c)* users' selection under the hot-spot guessing; *d)* comparisons with biometric authentication scheme.

a) Login and Registration Time: We recorded the time cost of participants spending on registration and authentication phase separately. Figure 6a illustrates that the new user needs more time for registration and login, with approximate 45 and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2019.2944301, IEEE Internet of Things Journal

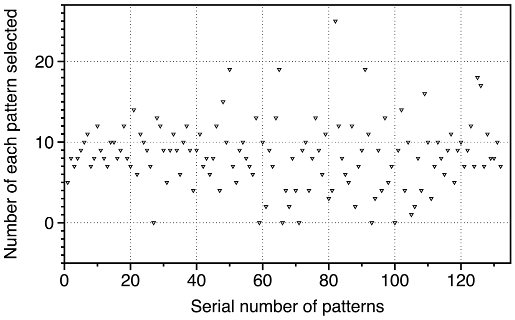


Fig. 7: The distribution of the number of the patterns selected.

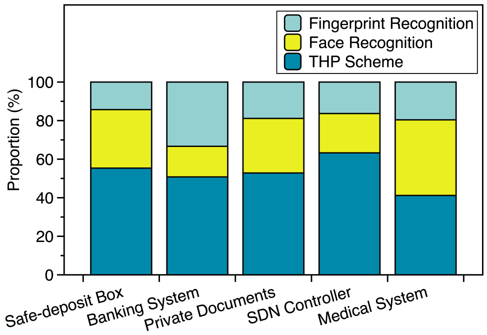


Fig. 8: Comparison with biometric authentication scheme.

36 seconds respectively. After some practices, the time can be reduced to 26 and 20 seconds respectively, and the skilled users require even less time.

b) Pattern Selection and Security Levels: The advanced strategies discussed in §III-B provides a flexible way to allow users to set the security levels for their system under various scenarios through changing the number of patterns. First, we asked the participants to perform the registration process. Figure 6b shows that 60% users selected 1 pattern for their authentication system, and the proportion decreased with the number of chosen patterns increase. Moreover, we surveyed the users' preferences of choosing the number of patterns in different scenarios and the statistics are shown in Figure 6c. It is found that the users would consider the security as the most important factor when the authentication scheme is used in a sensitive place such as a bank system and safe deposit box.

c) Selection Trend for Hot-spot Guessing: In this experiment, we investigated the users' preference of selecting patterns. We recorded the number of each pattern that was selected by users. As shown in Table VIII, 406 out of 677 participants selected 1 pattern, 155 participants selected 2 patterns, 81 participants selected 3 patterns, 32 participants selected 4 patterns, and 3 seclected 5 patterns, resulting in a total of $406\times1+155\times2+83\times3+32\times4+3\times5 = 1102$ patterns' options. The distribution of the number of the patterns selected is shown in Figure 7, where we have ordered each pattern in random. As it shown from the Figure 7, the number of patterns selected is relatively evenly, of which one pattern is selected more than 20 times, 6 patterns is not be selected, and the number of selected patterns is maintained within the range of $6 - 11$. According to the experiment's results, we consider that the hot-spot guessing cannot organize an effective attack because there is not exist a special pattern which is selected far more often than other patterns. We will continue to pay attention to the number of users' choices for these patterns in the future.

d) Comparison with Biometric Authentication Scheme: We also add users' preferences for THP and some current biometric schemes in some common application scenarios. We selected five scenarios with high security requirements and counted the proportion of users' selection under different scenarios. Figure 8 shows that THP has very high chance to be chosen in the scenarios that require high security.

VI. Chronicity experiment

In this experiment, we investigate the usability of our THP for long term usage. The evaluation considers the scenario that a user has not used his/her password for a period time; we then observe the impact of time for user's memory and habits of using THP.

A. Experimental Setup

a) Experimental Setting: We used the following indicators to comprehensively determine the long-term usability of THP program:

- Memory retention rate: the number of people keeping memory over the total number of participants.
- Selection preference: if the users keep their preferences of selecting patterns and advanced strategy?
- The changing rate of registration and login speed.

b) Participants: We invited 232 participants who have already involved in usability experiment. We asked them to use the original account password to re-login authentication to check if they can still remember their passwords. Each participant has 5 time to perform the login process. Then we count the the number of successful logins for each participant. In addition, we asked the participants who forget their passwords to do the registration again and then observe the change of their registration perferences. Table VIII shows the participants information.

B. Experimental Results and Analysis

According to the data we collected, 221 out of 232 participants can successfully log in for the first time, so the success rate is 95.26%. 230 participants can successfully log in within 5 times, and the success rate is 99.14%. Only two people failed to log in. In addition, the two participants who failed in to log in were asked to perform registration again. Both remain the same registration habit, selected the same number of *first password*. However, keeping the same habits does not mean the attacker can crack our system more easily. In our hypothesis, the user registration process is unknown to the attacker. Thus, the attacker have no idea if a user changes the number of *first password*. Based on the analysis above, our THP can provide users with long term memory, which is suitable for most IoT devices.

VII. Discussion & Conclusion

A. Discussion

Although THP can resist mainstream attacks and has significant performance, there are a few aspects need to be considered in the future work.

First, THP is still vulnerable to the Hot-spot Guessing Attack like [26] [43] [44] [45]. We support user-defined uploading of pictures, and set the pattern display mode in the registration process to random, avoiding the problem of "selection tendency". This can confuse the attacker and make him/her difficult to form an attack target. We still consider the case when the user's pattern password is set to 1. The attacker can guess the password when a picture includes a hot-spot area. In future work, we will study how to pick or generate the pictures that users will not have a preference of the pattern selection.

Second, since the login mode used in THP is still a graphical password mechanism, in essence, anyone who knows the password can successfully login to the system. There are still some security risks. Considering this point, our scheme can combine with the biometric recognition mechanism to enhance the security of a system.

Finally, we have proved that our THP scheme can achieve high security, when users choose multiple pattern passwords. However, it may reduce some usability. It is necessary to find a balance between security and convenience. For our scheme, we suggest choosing 2 pattern passwords, which can provide high security with reasonable time consumption. We also compare our scheme with the existing schemes in terms of attack resistance and portability as shown in Figure 9.

B. Conclusion

In this paper, we develop a new authentication scheme which is perfectly meet the security requirements of a SDN-based IoT network. The desired authentication scheme for a SDN-based IoT network must be able to prevent multiple attacks without losing too much usability. Our THP combines the graphic - based and text-based password to achieve two goals–high security and high usability. The high security is due to the design, implicitly transforming the passwords to a login indicator, which makes our method inmate with majority attacks, even the recording screen attack. The high usability benefits from the graphic-based scheme, which is easy to be remembered. We implemented the prototype of the THP scheme on Android and iOS platforms and conducted three types of experiments to comprehensively evaluate the scheme performance. Our evaluation involved 694 participants who performed 3096 login processes in 63 days. The experimental results demonstrate the high security and usability of our THP. Furthermore, we theoretically analyzed the security of our scheme, and then proposed an advanced strategy which allows the users dynamically set their passwords to meet various security requirements in different scenarios.

Acknowledgments

This work was supported by the National Key R&D Program of China under Grant 2017YFB0802300. This work was also partly supported by NSFC under No.61772466 and U1836202, the Zhejiang Provincial Natural Science Foundation for Distinguished Young Scholars under No.LR19F020003, the Provincial Key Research and Development Program of Zhejiang, China under No.2017C01055, and the Alibaba-ZJU Joint Research Institute of Frontier Technologies.

References

[1] IT168, "iphone has taken the fight to 3d printing by easily cracking android's face recognition feature," 2018, https://baijiahao.baidu.com/s?id=1620243794505991223\&wfr=spider\&for=pc.

[2] M. Kumar, T. Garfinkel, B. Dan, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," in *Symposium on Usable Privacy & Security*, 2007.

[3] T. Perković, M. Čagalj, and N. Saxena, *Shoulder-Surfing Safe Login in a Partially Observable Attacker Model*, 2010.

[4] E. Darbanian and G. D. Fard, "A graphical password against spyware and shoulder-surfing attacks," in *International Symposium on Computer Science & Software Engineering*, 2015.

[5] T. Kwon and J. Hong, "Analysis and improvement of a pin-entry method resilient to shoulder-surfing and recording attacks," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 2, pp. 278–292, 2017.

[6] M. Alsaleh, M. Mannan, and P. C. V. Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Transactions on Dependable & Secure Computing*, vol. 9, no. 1, pp. 128–141, 2011.

[7] W. Ding and W. Ping, *Offline Dictionary Attack on Password Authentication Schemes Using Smart Cards*, 2015.

[8] S. K. Sood, A. K. Sarje, and K. Singh, "Cryptanalysis of password authentication schemes: Current status and key issues," in *Proceeding of International Conference on Methods & Models in Computer Science*, 2010.

[9] A. Paivio, T. B. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?" *Psychonomic Science*, vol. 11, no. 4, pp. 137–138, 1968.

[10] S. Brostoff and M. A. Sasse, *Are Passfaces More Usable Than Passwords? A Field Trial Investigation*, 2000.

[11] A. D. Angeli, M. Coutts, L. Coventry, G. I. Johnson, D. Cameron, and M. H. Fischer, "Vip:a visual approach to user authentication," in *Proc Working Conference on Advanced Visual Interface*, 2002.

[12] B. Ives, "The domino effect of password reuse," *Communications of the Acm*, vol. 47, no. 4, pp. 75–78, 2004.

[13] J. Long, "No tech hacking a guide to social engineering, dumpster diving, and shoulder surfing," *Syngress Media U S*, 2008.

[14] T. Kwon, S. Shin, and S. Na, "Covert attentional shoulder surfing: Human adversaries are more powerful than expected," *IEEE Transactions on Systems Man& Cybernetics Systems*, vol. 44, no. 6, pp. 716–727, 2017.

[15] T. Kwon and S. Na, "Tinylock: Affordable defense against smudge attacks on smartphone pattern lock systems," *Computers & Security*, vol. 42, no. 4, pp. 137–150, 2014.

[16] S. Schneegass, F. Steimle, A. Bulling, F. Alt, and A. Schmidt, "Smudge-safe: Geometric image transformations for smudge-resistant user authentication," 2014.

[17] EvilLord, "Your phone is being secretly monitored so that others can see everything on the screen," 2018, https://baijiahao.baidu.com/s?id=1609433161910157135\&wfr=spider\&for=pc.

[18] A. Sheng, "Discover the most powerful android spyware, skygofree," 2018, https://baijiahao.baidu.com/s?id=1589809842021043922\&wfr=spider\&for=pc.

[19] N. Chakraborty, G. S. Randhawa, K. Das, and S. Mondal, "Mobsecure: A shoulder surfing safe login approach implemented on mobile device," *Procedia Computer Science*, vol. 93, pp. 854–861, 2016.

[20] K. R. Conger, "Uber's ios app had secret permissions that allowed it to copy your phone screen," *Gizmodo*, 2017.

[21] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in *Usenix Conference on Offensive Technologies*, 2010.

[22] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human - Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.

[23] X. Yu, W. Zhan, Y. Li, L. Liang, T. Z. Wen, and S. Li, “Evopass: evolvable graphical password against shoulder-surfing attacks,” *Computers & Security*, vol. 70, p. S016740481730113X, 2017.

[24] C. Castelluccia, M. Dürmuth, M. Golla, and F. Deniz, “Towards implicit visual memory-based authentication,” in *Network and Distributed System Security Symposium (NDSS)*, 2017.

[25] D. H. Nyang, H. Kim, W. Lee, S. B. Kang, G. Cho, M. K. Lee, and A. Mohaisen, “Two-thumbs-up: Physical protection for pin entry secure against recording attacks,” *Computers & Security*, pp. S0 167 404 818 305 789–, 2018.

[26] H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng, “A shoulder surfing resistant graphical authentication system,” *IEEE Transactions on Dependable & Secure Computing*, vol. PP, no. 99, pp. 1–1, 2018.

[27] T. V. Nguyen, N. Saebae, and N. Memon, “Draw-a-pin: Authentication using finger-drawn pin on touch devices,” *Computers & Security*, vol. 66, 2017.

[28] T. Takada, “Fakepointer: An authentication scheme for improving security against peeping attacks using video cameras,” in *Second International Conference on Mobile Ubiquitous Computing*, 2008.

[29] D. Kim, P. Dunphy, P. Briggs, J. Hook, J. Nicholson, J. Nicholson, and P. Olivier, “Multi-touch authentication on tabletops,” in *Sigchi Conference on Human Factors in Computing Systems*, 2010.

[30] S. Wiedenbeck, J. Waters, L. Sobrado, and J.-C. Birget, “Design and evaluation of a shoulder-surfing resistant graphical password scheme,” in *Proceedings of the working conference on Advanced visual interfaces*. ACM, 2006, pp. 177–184.

[31] H. Zhao and X. Li, “S3pas: A scalable shoulder-surfing resistant textual-graphical password authentication scheme,” in *International Conference on Advanced Information Networking & Applications Workshops*, 2007.

[32] Z. Zheng, X. Liu, L. Yin, and Z. Liu, “A stroke-based textual password authentication scheme,” in *International Workshop on Education Technology & Computer Science*, 2009.

[33] L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, “Against spyware using captcha in graphical password scheme,” in *IEEE International Conference on Advanced Information Networking & Applications*, 2010.

[34] V. Roth, R. Kai, and R. Freidinger, “A pin-entry method resilient against shoulder surfing,” in *Acm Conference on Computer & Communications Security*, 2004.

[35] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. D. Memon, “Authentication using graphical passwords: Effects of tolerance and image choice,” in *Symposium on Usable Privacy & Security*, 2005.

[36] N. Chakraborty and S. Mondal, “Color pass: An intelligent user interface to resist shoulder surfing attack,” in *Students Technology Symposium*, 2014.

[37] E. V. Zezschwitz, A. Koslow, A. D. Luca, and H. Hussmann, “Making graphic-based authentication secure against smudge attacks,” 2013.

[38] Y. Qiang, H. Jin, Y. Li, J. Zhou, R. H. Deng, Y. Qiang, Y. Li, and J. Zhou, “Designing leakage-resilient password entry on touchscreen mobile devices,” in *Acm Sigsac Symposium on Information*, 2013.

[39] N. H. Zakaria, D. Griffiths, S. Brostoff, and J. Yan, “Shoulder surfing defence for recall-based graphical passwords,” 2011.

[40] Runye, “Fingerprint unlock can also be broken,” 2018, http://baijiahao.baidu.com/s?id=1601780706643320115&wfr=spider&for=pc.

[41] IT168, “iphone has taken the fight to 3d printing by easily cracking android’s face recognition feature,” 2018, https://baijiahao.baidu.com/s?id=1620243794505991223\&wfr=spider\&for=pc.

[42] Amusi, “Biometric authentication under threat: Liveness detection hacking,” 2019, https://cloud.tencent.com/developer/article/1484902/.

[43] B. B. Zhu, J. Yan, G. Bao, M. Yang, and N. Xu, “Captcha as graphical passwords—a new security primitive based on hard ai problems,” *IEEE transactions on information forensics and security*, vol. 9, no. 6, pp. 891–904, 2014.

[44] S. Chiasson, P. C. Van Oorschot, and R. Biddle, “Graphical password authentication using cued click points,” in *European Symposium on Research in Computer Security*. Springer, 2007, pp. 359–374.

[45] J. Thorpe and P. C. V. Oorschot, *Human-seeded attacks and exploiting hot-spots in graphical passwords*, 2007.

Liming Fang received the Ph.D. degree in Computer Science from Nanjing University of Aeronautics and Astronautics in 2012, and has worked as a postdoctoral fellow in the information security from City University of Hong Kong. Now, he is an associate professor at the School of Computer Science, Nanjing University of Aeronautics and Astronautics. His current research interests include cryptography and information security. Liming Fang has published more than 50 paper in his field, including IEEE TDSC, IEEE TIFS, Theoretical Computer Science, Designs Codes and Cryptography, Information Sciences, etc.

Yang Li received the B.S. degree in Automation from Northwestern Polytechnical University in 2018, and is currently pursuing the M.S. degree in Cyberspace Security from Nanjing University of Aeronautics and Astronautics. His recent work has focused on artificial intelligence security and login authentication security.

Xinyu Yun received the B.S. degree in Computer from Nanjing University of Aeronautics and Astronautics in 2019, and is currently pursuing the M.S. degree in Computer from Nanjing University of Aeronautics and Astronautics. Her recent work has focused on artificial intelligence security and login authentication security.

Zhenyu Wen is currently a postdoc researcher at the School of Computing, Newcastle University, UK. He received M.S and Ph.D. degrees in computer science from Newcastle University, Newcastle Upon Tyne, UK in 2011 and 2015 respectively. His current research interests include multi-objects optimisation, big data processing and cloud computing.

Shouling Ji is a ZJU 100-Young Professor in the College of Computer Science and Technology at Zhejiang University and a Research Faculty in the School of Electrical and Computer Engineering at Georgia Institute of Technology. He received a Ph.D. in Electrical and Computer Engineering from Georgia Institute of Technology and a Ph.D. in Computer Science from Georgia State University. His current research interests include AI Security, Data-driven Security and Data Analytics. He is a member of IEEE and ACM and was the Membership Chair of the IEEE Student Branch at Georgia State (2012-2013).

Weizhi Meng is currently an assistant professor in the Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark. He obtained his Ph.D. degree in Computer Science from the City University of Hong Kong (CityU), Hong Kong. His primary research interests are cyber security and intelligent technology in security including intrusion detection, smartphone security, biometric authentication, HCI security, cloud security, trust management, malware detection, blockchain in security, cyber-physical system security and IoT security. He is a senior member of IEEE.

Zehong Cao is a Lecturer (a.k.a. Assistant Professor) with Discipline of Information and Communication Technology (ICT), School of Technology, Environments and Design, College of Sciences and Engineering, University of Tasmania (UTAS), Hobart, Australia, and an Adjust Fellow with School of Computer Science, Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), Australia. He received the dual PhD degree in Information Technology from UTS, and Electrical and Control Engineering from National Chiao Tung University (NCTU) in Taiwan. He received the MS and BS from The Chinese University of Hong Kong and Northeastern University, respectively. He serves as the Associate Editors of IEEE Access (2018 - Present) and Journal of Journal of Intelligent and Fuzzy Systems (2019 - Present), and the Guest Editor of IEEE Transactions on Emerging Topics in Computational Intelligence (2019), Swarm and Evolutionary Computation (2019), and Neurocomputing (2018). He had an ESI highly cited paper (2019) and a string of successful 30+ publications among the most respected journals, including Nature Scientific Data, IEEE Trans. Fuzzy Systems, IEEE Trans. Neural Networks and Learning Systems, IEEE Trans. Cybernetics, IEEE Trans. Systems, Man, and Cybernetics: System, IEEE Systems, Man, and Cybernetics Magazine, IEEE Trans. Biomedical Engineering, IEEE Access, International Journal of Neural Systems, Information Science, Neurocomputing, and Neural Computing and Applications. He was awarded UTS Centre for Artificial Intelligence Best Paper Award (2017), UTS Faculty of Engineering and IT Publication Award (2017), UTS President Scholarship (2015), and NCTU & Songshanhu Scholarship (2013). His research interests cover Fuzzy Sets and Systems, Fuzzy Neural Networks, Brain-Computer Interaction, Biosignal Processing, Game-based Machine Learning, and Data Mining.

M. Tanveer is Assistant Professor and Ramanujan Fellow at the Discipline of Mathematics of the Indian Institute of Technology, Indore. Prior to that, he spent one year as a Postdoctoral Research Fellow at the Rolls-Royce@NTU Corporate Lab of the Nanyang Technological University, Singapore. His research interests include support vector machines, optimization, applications to Alzheimer's disease and dementias, biomedical signal processing, and fixed point theory and applications. He has published over 25 referred journal papers of international repute. He is the recipient of the 2016 DST-Ramanujan Fellowship in Mathematical Sciences and 2017 SERB-Early Career Research Award in Engineering Sciences which are the prestigious awards of INDIA at early career level. He is a Senior Member of IEEE, editorial review board member of Applied Intelligence, Springer, lead Guest Editor of ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) and Associate Editor for IEEE SMC 2019. He has also co-edited one book in Springer on machine intelligence and signal analysis. He has also been organizer and invited speaker in many international conferences and Symposiums. He was the Co-Chair of Special Session Proposal in 2018 IEEE SSCI 2018. Tanveer is currently the Principal Investigator of 04 major research projects funded by Government of India including Department of Science and Technology (DST), Science & Engineering Research Board (SERB), Council of Scientific & Industrial Research (CSIR).

Appendix

Regarding the security experiment, usability experiment and chronicity experiment, we conducted a questionnaire survey on the participants after each experiment, and the questionnaire content is shown in table IX. In addition to the user's basic information, we also investigated the user's preference for this scheme. The investigation results of security experiment are shown in table VI, and the investigation results of usability experiment and chronicity experiment are shown in table VI. After the completion of the chronicity experiment, we asked 88 participants to complete the experiment again and recorded the change of users' habits. The results are shown in table VII.

TABLE VI: DETAILS OF SECURITY EXPERIMENT

	No.	Percent
Gender	**300**	**100%**
male	156	52%
female	144	48%
Age	**300**	**100%**
20 - 29	201	67%
30 - 39	82	27.33%
40 - 49	12	4%
50 - 59	5	1.67%
Profession	**300**	**100%**
Student	176	58.67%
Teacher	21	7%
Engineer	83	27.67%
Business	20	6.67%
Phone brand	**300**	**100%**
iPhone	51	17%
HUAWEI	74	24.67%
OPPO	20	6.67%
VIVO	29	9.67%
XIAO MI	41	13.67%
Samsung	48	16%
Others	37	12.33%
Number of participants	**300**	**100%**
Shoulder-surfing Attack	300	100%
Smudge Attack	20	6.67%
Recording Screen Attack	40	13.33%
Experimental time	**32**	**100%**
Shoulder-surfing Attack	16	50%
Smudge Attack	8	25%
Recording Screen Attack	8	25%
Number of people who completed	**300**	**100%**
Shoulder-surfing Attack	260	86.67%
Smudge Attack	40	13.33%
Recording Screen Attack	20	6.67%

TABLE VII: DETAILS OF CHRONICITY EXPERIMENT (AFTER 20 DAYS)

	No.	Percent
Gender	**232**	**100%**
male	116	50.0000%
female	116	50.0000%
Age	**232**	**100%**
20 - 29	89	38.3621%
30 - 39	76	32.7586%
40 - 49	38	16.3793%
50 - 59	29	12.5000%
Profession	**88**	**100%**
Student	101	43.5345%
Teacher	39	16.8103%
Engineer	63	27.1552%
Business	29	12.50000%
Phone brand	**232**	**100%**
iPhone	62	26.7241%
HUAWEI	57	24.5690%
OPPO	24	10.3448%
VIVO	19	8.1897%
XIAO MI	33	14.2241%
Samsung	16	6.8966%
Others	21	9.0517%
Forgetting situation	**232**	**100%**
Forgetting password	2	0.8621%
Not forgetting password	230	99.1379%
Change of usage habits situation	**2**	**100%**
Not change	2	100.0000%
Change the number of patterns	0	0.0000%

TABLE VIII: DETAILS OF USABILITY EXPERIMENT AND CHRONICITY EXPERIMENT

	First use		3 days after 1st batch		7 days after 2nd batch		31 days after 3rd batch	
	No.	Percent	No.	Percent	No.	Percent	No.	Percent
Gender	**694**	**100%**	**286**	**100%**	**217**	**100%**	**191**	**100%**
male	395	56.91%	137	47.90%	129	59.44%	113	59.16%
female	299	43.08%	149	52.10%	88	40.56%	78	40.84%
Age	**694**	**100%**	**286**	**100%**	**217**	**100%**	**191**	**100%**
20 - 29	482	69.45%	195	68.18%	163	75.12%	146	76.44%
30 - 39	137	19.74%	56	19.58%	32	14.75%	28	14.66%
40 - 49	46	6.62%	26	9.10%	18	8.30%	16	8.38%
50 - 59	29	4.18%	9	3.15%	4	1.84%	1	0.52%
Profession	**694**	**100%**	**286**	**100%**	**217**	**100%**	**191**	**100%**
Student	485	69.85%	179	62.59%	143	65.90%	134	70.16%
Teacher	46	6.63%	23	8.04%	13	6.00%	7	3.67%
Engineer	132	19.02%	63	22.03%	52	23.96%	43	22.51%
Business	31	4.47%	21	7.34%	9	4.15%	7	3.66%
Phone brand	**694**	**100%**	**286**	**100%**	**217**	**100%**	**191**	**100%**
iPhone	143	20.61%	64	22.38%	43	19.82%	31	16.23%
HUAWEI	142	20.46%	59	20.63%	40	18.43%	38	19.90%
OPPO	56	8.07%	42	14.69%	32	14.75%	32	16.75%
VIVO	38	5.48%	38	13.28%	37	17.05%	29	15.18%
XIAO MI	78	11.24%	46	16.08%	42	19.35%	44	23.04%
Samsung	39	5.62%	16	5.60%	9	4.15%	5	2.62%
Others	196	28.24%	21	7.34%	14	6.45%	12	6.28%
The number of people selecting patterns	**677**	**100%**	**251**	**100%**	**208**	**100%**	**167**	**100%**
1 pattern password	406	59.97%	159	63.35%	117	56.25%	110	65.89%
2 pattern passwords	155	33.90%	61	24.30%	60	28.85%	42	25.15%
3 pattern passwords	81	11.97%	17	6.77%	17	8.17%	9	5.39%
4 pattern passwords	32	4.72%	11	4.38%	11	5.29%	4	2.40%
5 pattern passwords	3	0.44%	3	1.20%	3	1.44%	2	1.20%
The number of people being cracked	**677**	**100%**	**251**	**100%**	**208**	**100%**	**167**	**100%**
Once	0	0%	0	0%	0	0%	0	0%
Twice	0	0%	0	0%	0	0%	0	0%
3 times	0	0%	0	0%	0	0%	0	0%
4 times	0	0%	0	0%	0	0%	0	0%
5 times	0	0%	0	0%	0	0%	0	0%

TABLE IX: The questionnaire

Question	Answer
What is your user name when you register?	
What is your phone number when you register?	
How old are you?	
What is your gender?	
What is your occupation?	
What is your mobile phone brand?	
How long do you use your smartphone?	
How many times a day do you unlock your phone?	
About THP, how many patterns do you prefer to secure for your mobile phone?	
About THP, how many patterns do you prefer to secure for your office computer?	
About THP, how many patterns do you prefer to secure for your smart home?	
About THP, how many patterns do you prefer to secure for your banking system?	
About THP, how many patterns do you prefer to secure for your safe-deposit box?	
What do you think of the usability of THP?	
About THP, are you willing to use it for a long time?	
About THP, is it cracked during use?	

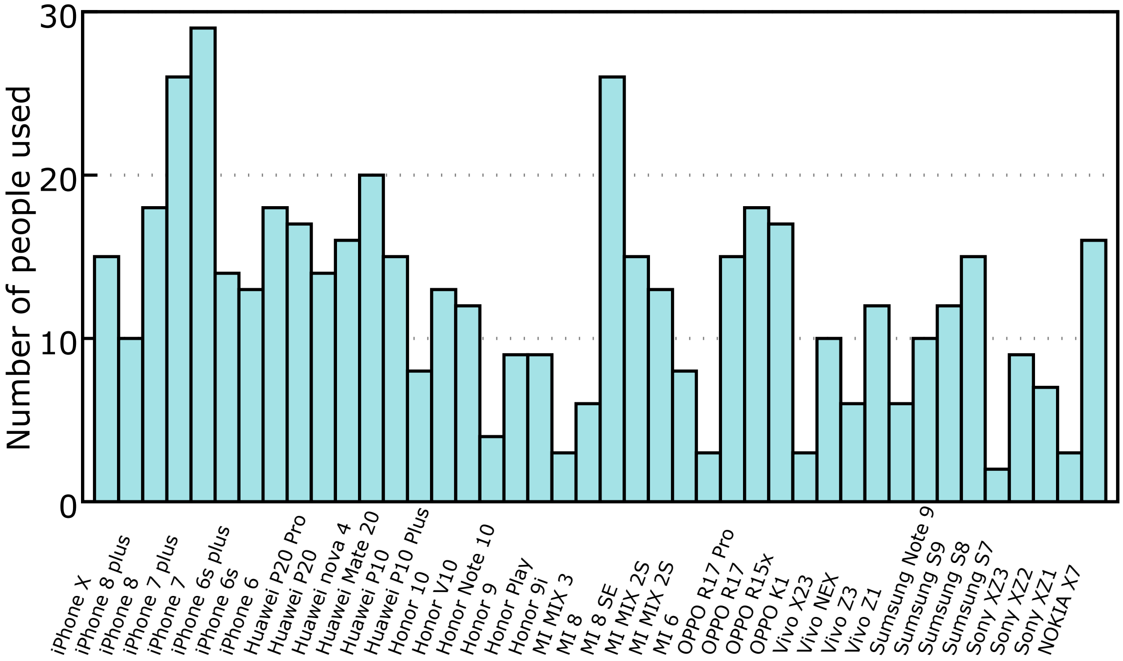


Fig. 9: Mobile phone statistics