Pattern of Success Vs. Pattern of Failure: Adaptive Authentication Through Kolmogorov–Smirnov (K-S) Statistics

Gahangir Hossain
Texas A&M University-Kingsville
Kingsville, TX, USA

Pradeep Palaniswamy
Texas A&M University-Kingsville
Kingsville, TX, USA

Rajab Challoo
Texas A&M University-Kingsville
Kingsville, TX, USA

***Abstract*—Smartphones have become a basic necessity in lives of all human beings. Apart from the core functionality of communication, these become a medium for storage of sensitive personal information, financial data and official documents. Hence, there is an inevitable need to emphasize on securing access to such devices considering the nature of data being stored. In addition, accessibility and authentication methods need to secure, robust, and user-friendly. This paper discusses an adaptive authentication mechanism with a nonparametric classification approach, Kolmogorov–Smirnov (K-S) statistic, which is coupled with the use of lock pattern dynamics as a secure and user-friendly two-factor authentication method. The data used for experimental exploration were collected from a systematically programmed Android device to capture the temporal parameters when individuals drew lock patterns on the touch screen. Each user has his individualistic way of drawing the pattern, which is used as the key for identifying imposters from valid users.**

Keywords—Mobile user experience; Biometrics; Smart mobile devices; Mobile identity management; Mobile authentication; Lock patterns; Mean time value

I. Introduction

The use of mobile smart devices for storing sensitive information and accessing online services has been increasing steadily. Mobile smart devices have become the one smart destination for all kinds of user data starting from social networking data [12] through mails (both personal and official) so on up to financial information. Despite all the information contained in a device and the transactions that can be performed with it, many users choose not to protect their devices, and at the same time they tend to be perpetually logged into some of the services provided by mobile third party applications. Thus, an attack on the mobile device or the loss can lead to undesired consequences such as the intrusion of privacy, the opportunity to impersonate users, and even severe financial loss.

Currently, most of the solutions that are designed for authenticating users into their mobile services are similar to authentication systems in mobiles. They usually use a PIN, a strong password, or some sort of extra external security token device. These techniques become cumbersome when applied to mobile devices and do not always provide a satisfactory user experience. Besides, they are not a sustainable approach for the future of mobile interactions, in which people would carry only one secure trustable device to perform most operations and would preferably use only one hand to operate such a device.

Pattern locking is another approach used in mobile smart devices with touch screen. Pattern locking refers to the option contained in the Android mobile platform [5] for locking the phone's screen. Pattern locks are graphical passwords that can be used to authenticate a user. Since it is a graphical approach users usually tend to remember the passwords better than a text-based pin. They also have the advantage that they can be easily drawn using a single hand ,giving much better user experience when compared to text-based passwords. However the enhanced user experience that comes with using a visualized password has its own setbacks. Unlike text-based passwords that are hidden when being typed pattern locks visible to eyes or video recording devices when they are being drawn. This makes pattern matched authorization more vulnerable to attacks.

As a generic solution to this issue, this paper discusses about enhancing the feature of pattern matched authorization by totaling its design with behavioral biometric features. The time taken by the user to draw the pattern, time taken between subsequent checkpoints in the pattern differs from user to user, this is considered as the behavioral biometric trait. The paper also hypothesizes that adding a biometric trait to lock pattern authorization can enhance the security of this type of graphical passwords by becoming a two-factor authentication mechanism.

II. Related Literature

As of now, research has been carried out on different approaches that provide an additional level of security for authenticating users both in mobiles as well as in desktops. There have been approaches where in users day to day activity can be used as a key for authenticating a user. As an example, a Smartphone might ask the user: “Today morning from who did you receive an SMS?” This type of authorization system has been discussed in [10].

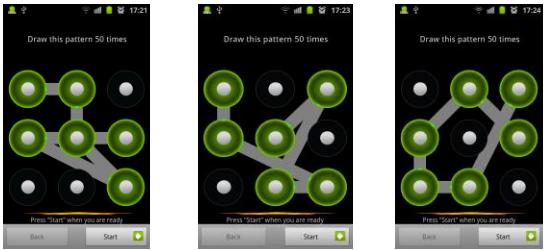
Another popular approach of identifying users is using key stroke dynamics. Keystroke dynamics or typing dynamics refers to the automated method of identifying or confirming the identity of an individual based on the manner and the rhythm of typing on a keyboard. Keystroke dynamics is a behavioral biometric. Specifically, most of the research done on the analysis of keystroke dynamics are for identifying users as they type on a mobile phone. Some can be found in [1], [2], [6], [7], [9] and others. One of these studies, [1], considers the dynamics of typed 4-digit PIN codes, in which the researchers achieved an average Equal Error Rate (ERR) 2 of 8.5%. However, the data for this experiment was collected using a mobile phone Handset interfaced to a PC through the keyboard connection "[1], thus their experiment does not portray real mobile situations neither does it consider typing PIN codes on touch-screens.

One of the mentioned studies, [9], partially considers the use of on-screen keyboards. The approach taken in this study however, has the disadvantage that the system has to be trained with a minimum of 250 keystrokes in order to achieve a low Equal Error Rate of approximately 2% which is not suitable for applications that do not require a lot of typing, neither for detecting short passwords or PIN intrusions.

Imposing the use of alphanumeric passwords on mobile devices creates the problem that users tend to choose simpler, weaker or repetitive passwords [7], since complicated strong passwords are harder to type on smaller on-screen keyboards. Therefore, suggestions for more unobtrusive methods for authentication on mobile smart phones have emerged as an alternative to typed passwords, such as gait biometrics (achieving an EER of 20.1%) [4] [8], or the unique movement users perform when answering or placing a phone call (EER being between 4.5% and 9.5%) [3]. Although these methods seem to be a promising approach towards enhancing the user experience, they require users to take the explicit actions like answering phone calls in order to be effective. Therefore, they are not fully suitable for scenarios when a user needs to interact or look at the phone in order to login to a mobile application or Online service. Besides, these methods only provide a one-factor authentication mechanism.

To the best of our knowledge, only one approach [11] deals with the use of biometric traits over a pattern matching authorization technique. In this approach the author would have compared various anomaly detectors (i.e., Euclidian detector, random forest, etc.) to find and compare the EERs and standard deviations of the techniques.

In our we use the same data set that was used in [11],the data collection is done using Google's platform for mobile devices, Android [5], we use a mobile application to collect data from different individuals on the way they draw lock patterns, their experience while doing so and other contextual factors., test participants were asked to draw three different lock patterns correctly a certain number of times (n=50 trials for each pattern), with each pattern consisting of six dots, as shown in Figure 1. More specifically, during a test session test participants were first shown an animation on how to draw the first lock pattern (see Figure 1(a)), once they had learnt it they were asked to draw that pattern correctly 50 times. They were then shown the second pattern (Figure 1(b)) and were also asked to draw it 50 times, and the same was done for the third pattern (Figure 1(c)). A static approach was used in which all participants drew the same three patterns, i.e., the input was identical for all tests [1]. Analogous to earlier keystroke studies (in which different distinguishing features are used, such as key holding time and digraphs [9]), two main features were captured for each successful trial: the *finger-in-dot* time, which is the time in milliseconds from the moment the participant's finger touches a dot to the moment the finger is dragged outside the dot area, and the *finger-in-between-dots* time, representing the speed at which the finger moves from one dot to the next. All erroneous trials were disregarded.


17:21
Draw this pattern 50 times
Press "Start" when you are ready
Back
Start
17:23
Draw this pattern 50 times
Press "Start" when you are ready
Back
Start
17:24
Draw this pattern 50 times
Press "Start" when you are ready
Back
Start

(a)1st Lock pattern (b) 2nd Lock pattern (c)3rd Lock pattern

Fig. 1. The three lock patterns that participants were asked to draw

After pattern unlocking experiment is designed, the data is collected that contains pattern matching timings for 32 users for three patterns. Each pattern is attempted to be drawn right 50 times. There are 11 temporal parameters (six time_on_dot timings and 5 five time_between_dot timings) that were recorded in this experiment during every single trial.

III. Method

The basic purpose of an authentication system is to block the invalid access from the valid access. A commonly used authentication technique separates the invalid pattern from the valid pattern of using response time as modulators with minimum mean squared errors. However, whenever a user’s tapped lock pattern becomes similar (but not same) to the acceptable lock pattern, system might allow user to access the system and update the variance of lock pattern. This can be considered as adaptive lock pattern, or adaptive authentication. This adaptation process is explained with a block diagram as figure.

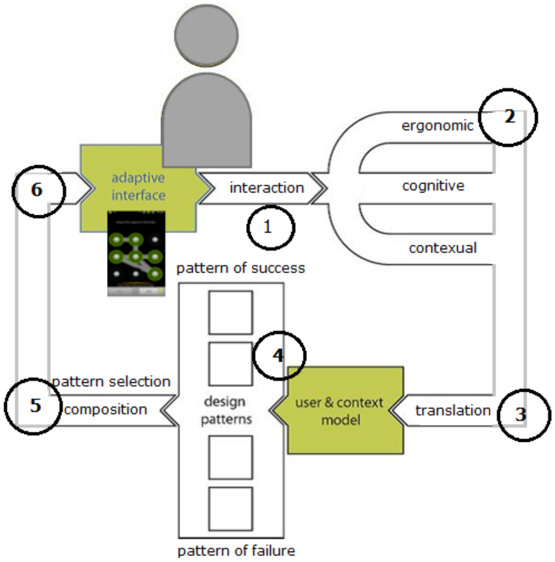


Fig. 2. A schematic representation of adaptive authentication with a pattern of success and a pattern of failure. Circles indicate the steps of the authentication and updating process

Step 1: User type lock pattern

Step 2: ergonomic, cognitive and contextual factors are applied to the patter to modulate it.

Step 3: The modulated signal is translated to the user and context model (personalized profile).

Step 4: Pattern is matched (with K-S test)

Step 5: Pattern is selected and composed to the adaptive model.

A formal model of an adaptive authentication system is shown in figure 3.

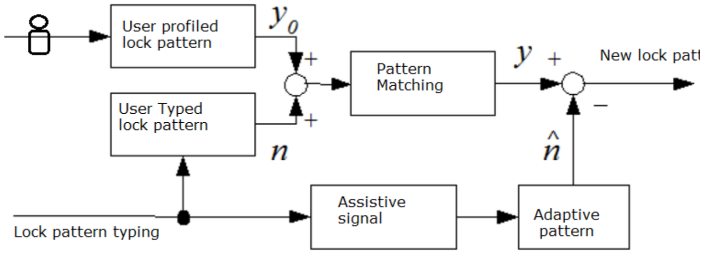


Fig. 3. A formal model of adaptive authentication

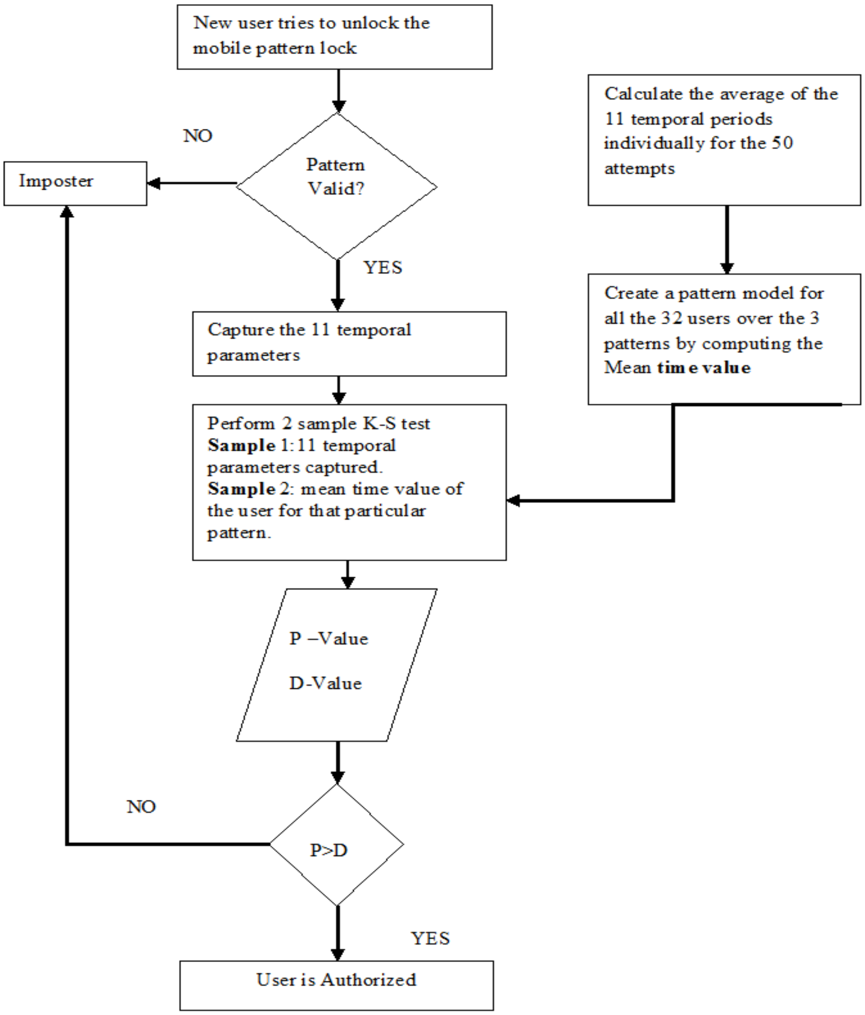

New user tries to unlock the mobile pattern lock
NO
Imposter
Pattern Valid?
YES
Capture the 11 temporal parameters
Calculate the average of the 11 temporal periods individually for the 50 attempts
Create a pattern model for all the 32 users over the 3 patterns by computing the Mean time value
Perform 2 sample K-S test
Sample 1: 11 temporal parameters captured.
Sample 2: mean time value of the user for that particular pattern.
P –Value
D-Value
NO
P>D
YES
User is Authorized

Fig. 4. Adaptive authentication analysis flow diagram

Figure 3, the formal model is a schematic representation of the flow of events that take place in pattern based cognitive authentication system. When a new user tries to enter into the system by swiping the lock pattern, if the attempted pattern was drawn right then we capture the 11 temporal parameters (i.e, 6 time_on_dot timings and 5 time_between_dot timings).We also have a pattern model of composed of a matrix [96*11](96-32 users * 3 patterns,11- temporal parameters) of mean time values. Based on the user and the pattern we choose the corresponding mean time value (i.e., corresponding row) from the pattern model. Next we perform a KS test on both these samples to derive the P and D values. If the P-value is greater than the D-value then the user is an authorized user, else the user is considered as an imposter and is requested to repeat the process. A complete flow diagram of the pattern matching is shown in figure 4.

IV. Pattern of Success Vs. Failure

The proposed design is a logical extension of the technique handled in [11]. Non-parametric tests are performed in-order to determine whether the sequence of moves made by the user to unlock a pattern matches statistically with the pattern recorded on the system. A non-parametric test is one in which there are no pre-requisite on the data that is to be processed, i.e. There is no emphasis that the data must follow a particular distribution.

A. *The Kolmogorov–Smirnov Test*

The **Kolmogorov**–**Smirnov** test (commonly known as a K–S test or **KS** test) is a nonparametric test of the equality of continuous, one-dimensional probability distributions that can be used to compare a sample with a reference probability distribution or to compare two independent samples. Since two temporal parameters need to be compared a two sample K-S test is used.

The temporal data for the legitimate user's (i.e. the user the system is trained to accept) attempts is averaged out and considered as the first sample.

When a user tries to access the system by drawing the unlocking pattern, the temporal values for the attempt are captured and considered as the second sample.

The two samples are compared using K-S test so as to determine whether they belong to the same distribution (i.e. prove whether they are statistically similar). On a contrary, if the samples are statistically dissimilar we can say that the user is an imposter.

A classic example to explain the scenario is the summary of a cricket match, how can one determine whether the pattern of the chase is similar?

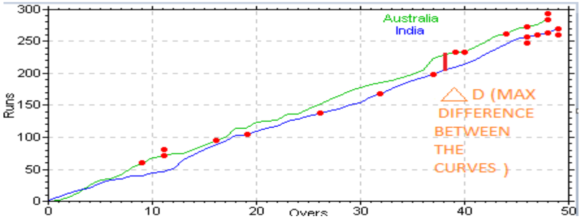


Fig. 5. Example score patterns from a cricket match

The deviation in chase patterns can be captured by analyzing delta D, lesser the value similar the pattern. K-S test follows a similar approach.

The Kolmogorov–Smirnov statistic quantifies a distance between the empirical distribution functions of two samples. K-S test computes the maximum absolute distance between the two cumulative functions. The null distribution of K-S test is calculated under the null hypothesis that the samples are drawn from the same distribution (two-sample case).

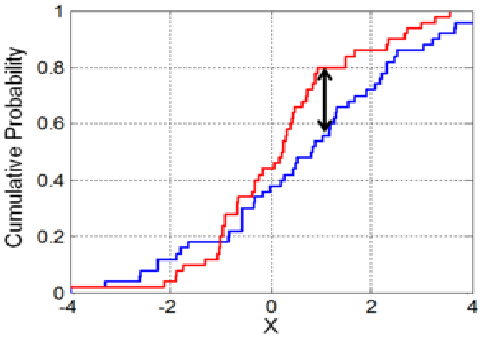


Fig. 6. Example of a K-S test (2 Sample)

Figure 5 portrays the example score pattern (Given in figure 6) in terms of cumulative probability.

B. *Kolmogorov–Smirnov (K-S) statistic*

The Kolmogorov–Smirnov (K-S) statistic for a two sample test is defined as

$$Dn, n' = \sup |F1, n(x) - F2, n'(x)|$$

Where F1,n and F2,n' are the empirical distribution functions of the first and the second sample respectively. Sup is the supremum[12] function. The null hypothesis is given by

$$Dn, n' > Pn, n'$$

Where P n,n' is given by

$$Pn, n' = c(\alpha)\sqrt{n + n' /}\sqrt{n. n'}$$

The value of c(α) is given in the table below for each level of α.

TABLE I. Range of Significance Levels

α	0.10	0.05	0.025	0.01	0.005	0.001
$c(\alpha)$	1.22	1.36	1.48	1.63	1.73	1.95

The level α is the "significance level" of the test, the rate of Type I error, the probability of detecting a difference under the assumptions of the null hypothesis (that the two samples are drawn from the same distribution).For our experiment we assume c(α) to be 0.05.

V. Metrics and Computation

A. *Types of errors*

False rejection rate (Type I error): The false rejection rate or FRR is the probability that the system incorrectly rejects access to an authorized person, due to failing to match the biometric input with a template.

False acceptance rate (Type II error): The false acceptance rate or FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's far typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

B. Mean Time Value

Mean time value of a particular user drawing a particular pattern is the average time that the particular user might take to complete drawing the pattern. Mean time value is calculated by simple computing the mean of all the 11 temporal parameters individually for all the 50 attempts made by the user drawing the pattern. Resultant would be a set of 11 normalized temporal parameters.

C. False Acceptance Rate

FAR is computed for each user by selecting the mean time value for a user and then conducting a K-S test against all other user samples obtained (31 other users for their 50 attempts).This is termed as a Set and each set consists of (31*50) K-S tests . 32 Sets are obtained by repeating the procedure for all the 32 users. The resulting data set would contain 992 comparisons (32 *31 users).The number of tests that has failed the null hypothesis is then computed for each user individually in order to compute the FAR value (i.e., more tests failed lesser the false acceptance).

D. False Rejection rate

In order to compute the false rejection rate of a particular user in a particular Patten, Mean time value of that particular user is tested against the 50 samples for the same user. The same procedure is repeated for all 32 users. In case of FRR computation the number of tests that failed the null hypothesis is directly proportional to FRR value.

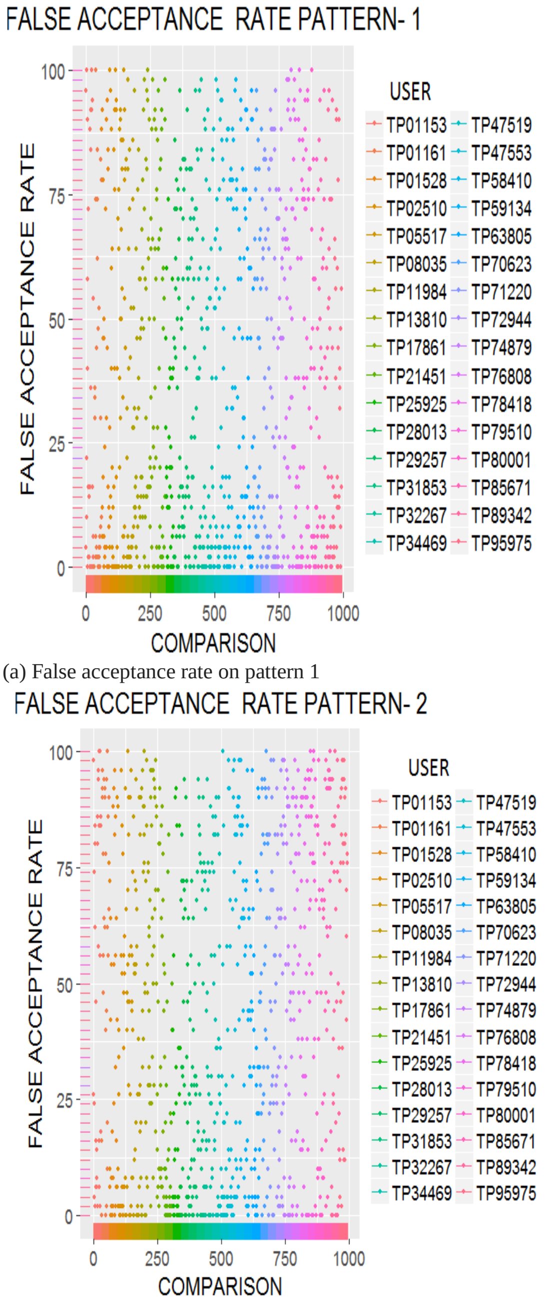
VI. Results

We summarize the results in the tabular column given in Table 2.

TABLE II. Overall Comparison of False Acceptance Vs. False Rejection Rates for the Three Patterns Used

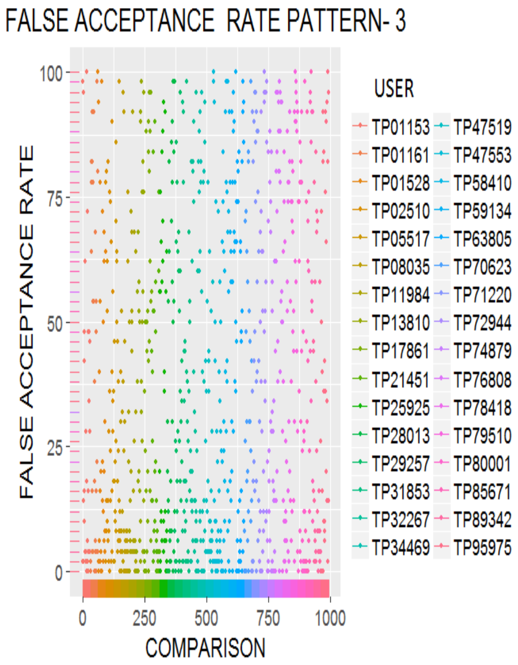
PATTERN	FALSE REJECTION RATE	FALSE ACCEPTANCE RATE
pattern 1	17	38.32258
pattern 2	13.4375	43.14516
pattern 3	14.5625	36.38508

The overall results are pictorially summarized as follows. There are three patterns and for each pattern both FAR and FRR are calculated.



(a) False acceptance rate on pattern 1

(b) False acceptance rate on pattern 2



(c) False acceptance rate on pattern 3

Fig. 7. (a) False acceptance rate on pattern 1 (b) False acceptance rate on pattern 2 (c) False acceptance rate on pattern 3

A. Inference

Figures 7 (a) (b) and (c) make it evident that in most Cases the incorrect acceptance rate is lesser than 15. However, there are outliers reaching up to peaks. To be specific, there is 100% fault acceptance rate between users "TP01153" "TP02510" while drawing pattern 1. While having a closer look at this issue it can be observed that when the two users are KS-Tested against each other a D value comparatively smaller to P value is obtained (i.e.: D = 0.25, p-value = 0.8475).This has resulted because the timing patterns of these 2 users closely matches with each other . This infers that the users have very similar pattern of drawing. It can be also absorbed that these 2 users have very high false acceptance rates on other 2 patterns as well (Pattern 2 is 74% and pattern3 is 96%).

With respect to false rejection it can be observed that the false rejection rate, it is usually below 20 % .However there are few spikes in FRR graph as well. When examined it is evident that user TP11984 has a false rejection rate of 88% on pattern 1 .On closer observation it is clear that the user's swipe times undergoes a wide range of oscillations . For example a temporal parameter (time_on_dot1) values ranges from 65 to 506 mille seconds. These in constancies follow throughout the pattern leading to a very false high false rejection rate (pattern of success). This is shown in figure 8.

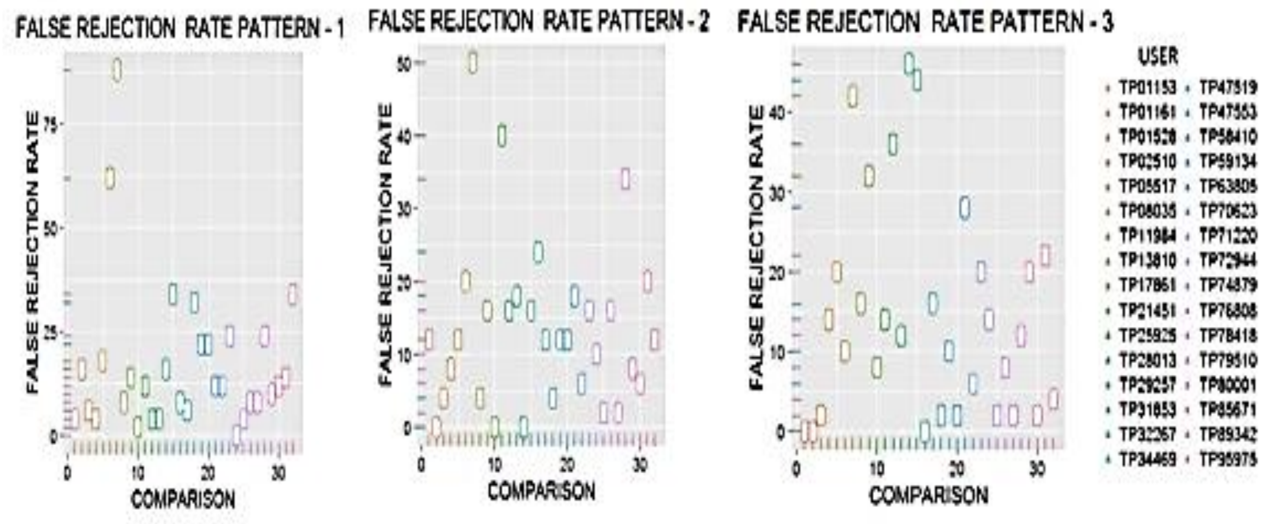


Fig. 8. False rejection rate across the 3 patterns

VII. Conclusion

K-S test is a simple but effective nonparametric test that can be used in order to determine whether 2 Radom samples belong to the same distribution. Hence, it is useful pattern of success and pattern of failure identification. As K-S test compares the overall distributions rather than specifically locations or dispersions, the test is a useful adaptive classification tool. Though the failures in results are justified to a certain extent we cannot deny the fact that the proposed method needs improvement, alternative choices for non-parametric tests include multivariate [13] and multidimensional [14] K-S test. Another, improvement that can be considered is for calculating the mean time value for a particular user against a pattern. In the current approach, we just compute a normal average of all the values, whereas we can do much better than that. The pitfall in calculating the average is that, we will not be able to eliminate the outliers. By eliminating the outliers could improve the result of the computation by a great extent.

Though the two factor authorization mechanism is an effective one there were various inconsistencies those were observed as outliers when calculating the FRR and the FAR value. An effective approach to reduce such inconsistencies can be implemented by reducing the distance between checkpoints. In current scenario there are 6 checkpoints to obtain the temporal parameters. However, if the distance between check points is decreased the number of temporal parameters will increase, for example if the distance between check points is reduced by 50% the number of temporal parameters will increase by 50%. Increased number of temporal parameters will result in higher precision of results.

REFERENCES

[1] Clarke, N.L., Furnell, S.: Authenticating mobile phone users using keystroke analysis .Int. J. Inf. Sec. 6(1), 1{14 (2007).

[2] Clarke, N.L., Karatzouni, S., Furnell, S.: Flexible and transparent user authentication for mobile devices. In: SEC. pp. 1{12 (2009).

[3] Conti, M., Zachia-Zlatea, I., Crispo, B.: Mind how you answer me!: transparently Authenticating the user of a Smartphone when answering or placing a call. In:Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. pp. 249-259. ASIACCS '11, ACM, New York, NY, USA (2011).

[4] Derawi, M.O., Nickel, C., Bours, P., Busch, C.: Unobtrusive user-authentication on mobile phones using biometric gait recognition. In: Proceedings of the 2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. pp. 306{311. IIH-MSP '10, IEEE Computer Society, USA (2010).

[5] Google: Android: Android - open source project (June 2011), http://source.android.com/

[6] Karatzouni, S., Clarke, N.L.: Keystroke analysis for thumb-based keyboards on mobile devices. In: SEC. pp. 253{263 (2007).

[7] Nauman, M., Ali, T.: TOKEN: Trustable Keystroke-Based Authentication for Web-Based Applications on Smartphones. In: Bandyopadhyay, S.K., Adi, W., Kim, T.h., Xiao, Y. (eds.) Information Security and Assurance, Communications in Computer and Information Science, vol. 76, pp. 286{297. Springer Berlin (2010).

[8] Nickel, C., Derawi, M.O., Bours, P., Busch, C.: Scenario test of accelerometer-based biometric gait recognition. In: Security and Communication Networks (IWSCN). 3rd International Workshop, Gj_vik, Norway (2011).

[9] Zahid, S., Shahzad, M., Khayam, S., Farooq, M.: Keystroke-based user identification on smart phones. In: Kirda, E., Jha, S., Balzarotti, D. (eds.) Recent Advances in Intrusion Detection, Lecture Notes in Computer Science, vol. 5758, pp. 224{243.Springer Berlin / Heidelberg (2009).

[10] Sourav Kumar DandapatIIT Kharagpur, India,Swadhin Pradhan,UTAustin, USA,Bivas MitraIIT Kharagpur, India.Romit Roy Choudhury,UIUC, USA.,Niloy Ganguly,IIT Kharagpur, India ., ActivPass: Your Daily Activity is Your Password Proceeding CHI '15 Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems Pages 2325-2334 ACM New York, NY, USA ©2015.

[11] Exploring Touch-screen Biometrics for UserIdentication on Smart Phones Julio Angulo and Erik WastlundKarlstad University,Universitetsgatan 2, 651 88 Karlstad, Swedenfjulio.angulo , erik.wastlundg@kau.sehttp://www.kau.se Aviv, A.J., Gibson, K., Mossop, E., Blaze, M., Smith, J.M.: Smudge attacks on smartphone touch screens. In: Proceedings of the 4th USENIX conference on Offensive technologies. pp. 1{7. WOOT'10, USENIX Association, Berkeley, CA, USA(2010).

[12] The supremum (abbreviated sup;pural sup-rema) of a subset S of a partially ordered set T is the least element in T that is greater than or equal to all elements of S, if such an element exists. Consequently, the supremum is also referred to as the least upper bound (or LUB) https://en.wikipedia.org/wiki/Infimum_and_supremumA. Alpher, , and J. P. N. Fotheringham-Smythe. Frobnication revisited. Journal of Foo, 13(1):234–778, 2003.

[13] Justel, A.; Peña, D.; Zamar, R. (1997). "A multivariate Kolmogorov–Smirnov test of goodness of fit". Statistics & Probability Letters 35 (3): 251–259. doi:10.1016/S0167-7152(97)00020-5.

[14] Fasano, G., Franceschini, A. (1987). "A multidimensional version of the Kolmogorov–Smirnov test". Monthly Notices of the Royal Astronomical Society 225: 155–170. Bibcode:1987MNRAS.225..155F. doi:10.1093/mnras/225.1.155. ISSN 0035-8711.