Jurnal Ilmu Komputer dan Informasi (Journal of Computer Science and Information)
17/1 (2024), 97-108. DOI: http://dx.doi.org/10.21609/jiki.v17i1.1235

Rethinking Smart Keyboard Layout to Aid Strong Password Creation

Md. Faruk Hossain[1], Md. Mizanur Rahman[2], Sarker Tanveer Ahmed Rumee[1,3], Moinul Islam Zaber [1,3,4]

[1] Department of Computer Science and Engineering, University of Dhaka, Bangladesh
[2] University of Tsukuba, Tsukuba, Ibaraki 305-8577, Japan
[3] Data and Design Lab, University of Dhaka, Bangladesh
[4] United Nations University, Guimarães, Portugal

Email: fhossain615@gmail.com, s2240177@u.tsukuba.ac.jp, rumee@cse.du.ac.bd, zaber@du.ac.bd

Abstract

In an era marked by increasing digitization and the omnipresence of smartphones, the importance of robust password security cannot be overstated. With the ever-growing threat of cyberattacks, there is a pressing need for user-friendly tools that facilitate the creation of strong and unique passwords. Traditional alphanumeric keyboard layouts (physical or virtual) have remained largely unchanged for decades, relying on the same QWERTY layout initially designed for typewriters. However, these layouts may not be optimal for generating strong passwords. This paper focuses on tailoring virtual keyboard layouts on smartphones specifically for strong password creation. For this, we have performed extensive user surveys to see if the presence of dedicated rows for digits and special characters (essential in any strong password) allows users to create stronger passwords compared to regular smartphone keyboard layout. Apart from that, we also investigated the optimal assignment of characters, digits, and special characters and their groupings in a single soft key. The findings from the detailed user experiment suggested optimal settings for a smartphone virtual keyboard (for Android) like- diagonal length for good typing speed (approximately between 8.38 and 9.41 cm), and key density (0.88 to 1.21 $keys/cm^2$) which produces the least error without sacrificing the strength of passwords created using those layouts. We hope the outcome of this paper will help designers to aid virtual keyboard layouts for smartphones that can motivate and create strong passwords without sacrificing usability.

Keywords: *Smartphone Keyboard, Strong Passwords, User Study, Key Layout, Typing Error*

1. Introduction

User authentication [1] is one of the first lines of defense against privacy violations and a cornerstone of any secure system. Numerous authentication schemes have been used for a long time, such as - graphical patterns, textual passwords, image-based passwords, fingerprint and iris scanners, face and voice recognition, security questions, phone-based two-factor authentication, etc [2–4]. However, a textual password-based authentication scheme remains the most popular form of user authentication. There is little chance that the scenario might change shortly [5]. With the rapid and wide-scale adoption of smartphones, researchers have put in new thoughts and ideas on how to design interfaces that ensure password security without sacrificing usability. However, this task is not straightforward and the focus of this research [6].

In traditional devices like computers or laptops, the keyboard is large enough for users to easily reach all the different types of letters, digits, and symbols. On the contrary, smartphones are input constraint devices and screen sizes are often very small. As a result, the keyboard layout that pops up when the user is typing on mobile devices generally consists of a selected set of characters. Other characters can be loaded by changing the on-screen layout 2 or 3 times. For example, accessing a specific symbol may require changing different pages which is frustrating for the user. Due to this limitation of the virtual keyboard, key size and the navigation requirement

between key pages make the text entry in the smartphone error-prone [7, 8]. Different vendors come up with custom virtual keyboards with different layouts which makes it even more difficult for the user to select strong passwords compared to regular computers. This implies the tendency to form weaker textual passwords among smartphone users, which makes the passwords more vulnerable in case of guessing or dictionary attacks.

To solve this problem, there has been a steady effort from the research community. Existing work like [9], demonstrates the need for an improved layout for the virtual keyboard in smartphones, which at the same time encourages the creation of stronger passwords and at the same time user friendly. This work performs a comprehensive user study on the virtual keyboard layout, alphanumeric and special character placements in the layout, and their corresponding counts on each key page. Survey results show important insights into this perspective and give useful direction for secure yet usable smartphone keyboard layout design.

The security of the authentication process relies on the strength of the passwords. Some studies have found that entering text using touchscreen devices affects typing and results in passwords with significantly lower entropy [9, 10]. An attacker can steal sensitive personal data from the database by cracking the passwords. Weak textual passwords are vulnerable to dictionary attacks or trillions of guesses. Also, It was examined that the textual password entry on mobile devices which is fraught with usability problems due to the size and input constraints of mobile devices[9]. The main motivating issue here is:

1) The keyboard layouts of the existing smartphones create frustration amongst the user because of the limitation of the screen size. For this reason, users tend to create weaker passwords that are vulnerable to attackers.
2) Smartphone use is increasing day by day. Soon, it might happen that all the personal data and transactions are being done with a smartphone. Therefore for security concerns, there should be a device new technique that will increase the strength of the textual passwords while keeping the usability of the technique.

The motivation implies the need for research in the area of generating strong and usable textual passwords in input-constrained devices like a smartphone.

From the perspective of strength, a good password is a combination of letters, symbols, and special symbols. Inserting special symbols in between the letters for smartphones is not as straightforward as the traditional devices. This can be explained with an example. iPhone is a popular smartphone brand and there is a significant amount of users who use the default keyboard of the iOS (operating system of iPhone) as the primary input entry method. Now, if a person needs to put a number in between two letters of the password, he/she needs to change the layout of the keyboard. For accessing some special symbols it may require changing two pages of the keyboard. This is frustrating for the users who may eventually generate a weak password.

Therefore, it is clear that keyboard layouts often influence the textual password construction in smart devices. Due to the lack of comfort with changing layouts, the strength of the passwords varies, because different people exercise these options differently. It is also a well-established fact that people want to select an easier password on smartphones and the current layout schemes encourage the user to do that. So, this work wants to devise novel ideas for the smartphone keyboard layout option, which will increase password strength and usability.

Major contributions of this work are listed below:

- A detailed comparison and user study (based on secure textual password construction) of the currently used smartphone keyboard layouts are done.
- Next, the above-mentioned surveys are repeated for several customized keyboard layouts, analyzing the usability issue when the keyboard size is changed to mitigate the strength and usability issues.
- Proposed novel criteria for positioning the keys in smartphone virtual keyboard, which encourages users not to select trivial passwords without sacrificing usability and password strength.

The rest of the paper is organized as follows: Section 2 talks about the preliminary concepts and key terminologies. Then, Section 3 discusses a few closely related works. In section 4, we discussed the details of the proposed system: user data collection, candidate keyboard layout design, evaluation, user experiment, and findings on those candidate layouts to find the optimal arrangements. Threats to the Validity of the methods and experiments done in this work are discussed in section 5. Finally, section 6 concludes the paper with a summary of the findings of this work, its limitations, and a discussion on possible future work.

2. Background

This section introduces a few key concepts and terminologies relevant to our work.

2.1. User authentication in smartphones

Smartphones are becoming more and more innovative every day. Nowadays most phones are equipped with many sensors like touchscreen, microphone, gyroscope, motion sensor, etc. that can be a source of user authentication. However, on the user side, the phone screen (through the virtual keyboard, touches, and hand gestures) is the primary method to interact with the device [11]. A few authentication measures are discussed below.

At its core, we have the trusty *PIN* or *Password*, a digital key to our world that's been a staple for years. Its simplicity is its strength, but as technology advances, so do our options.

Biometric authentication methods have taken center stage. Fingerprint recognition, for instance, has become a favorite due to its quick and convenient nature. A simple touch and the phone is yours. Facial recognition is another standout, using the front camera to create a unique map of your face, ensuring your device knows you instantly.

For those seeking a higher level of security, there's iris scanning, which captures the intricate patterns in your irises. Voice recognition listens to your unique vocal patterns, though it's not as common due to its sensitivity to external factors.

Pattern lock offers a touch of nostalgia, as you create a secret design on the screen to unlock your device. It's playful but may not be as secure as some of the biometric options. Meanwhile, palm vein scanning takes personal identification to the next level, analyzing the vein patterns in your palm.

For those who require the utmost security, *multi-factor authentication* combines two or more of these methods, fortifying your device against unauthorized access.

Lastly, there's *behavioral biometrics*, which observes your unique habits and patterns, such as typing speed and style, to silently authenticate your identity without the need for explicit actions.

These authentication methods tell a story of innovation, adaptation, and the ongoing pursuit of a seamless yet secure smartphone experience. It's a world where our very presence unlocks the magic of our digital lives, and our device becomes not just smart but our trusted guardian.

2.2. Keyboard Layout Design Issues

Researchers made a significant effort to design soft keyboards for mobile phones from the full-length QWERTY keyboard through extensive usability analysis. Following are some of the key design issues that dictate a particular soft keyboard layout.

The *size* and *spacing of keys* on the virtual keyboard are crucial for accuracy and ease of use. Keys should be large enough to prevent frequent mistypes, and there should be adequate spacing between keys to minimize accidental taps on adjacent keys.

The distance between keys, measured diagonally, impacts the comfort and usability of the keyboard. Keys that are too far apart can strain users' fingers and slow down typing.

With increasing screen sizes in smart devices (phones and tablets), a variety of arrangements of keys have emerged in the case of layout design. However, now the screen size variations are also higher contributing to the trade-off in soft key layout planning [12].

Allowing users to customize the keyboard layout can enhance their experience. This may include options for adjusting key size, layout, and the inclusion of special characters or symbols that are frequently used by the individual.

Many users require keyboards that support multiple languages. Designing a keyboard that can seamlessly switch between different language layouts or provide predictive text suggestions in multiple languages is a challenge.

2.3. Ease of Use Factors

The pressing of a key in a virtual keyboard of a smartphone is counted as one keystroke. Even if the input is wrong the keystroke is counted. *Keystroke time* denotes the average time in seconds needed for a key press.

The number of backspaces used to delete the wrongly entered character of a textual password is counted as the total number of errors. *Error Rate* represents the ratio of this number to total valid key presses (characters present in the target password).

3. Related Work

Researchers have made significant efforts to improve user authentication in mobile devices. Here we discuss a few closely related works that primarily focus on the smartphone soft keyboard layouts and their effect on users. There is a handful of prior work on textual password generation from the smartphone. Bao et al. report that smartphones have significantly

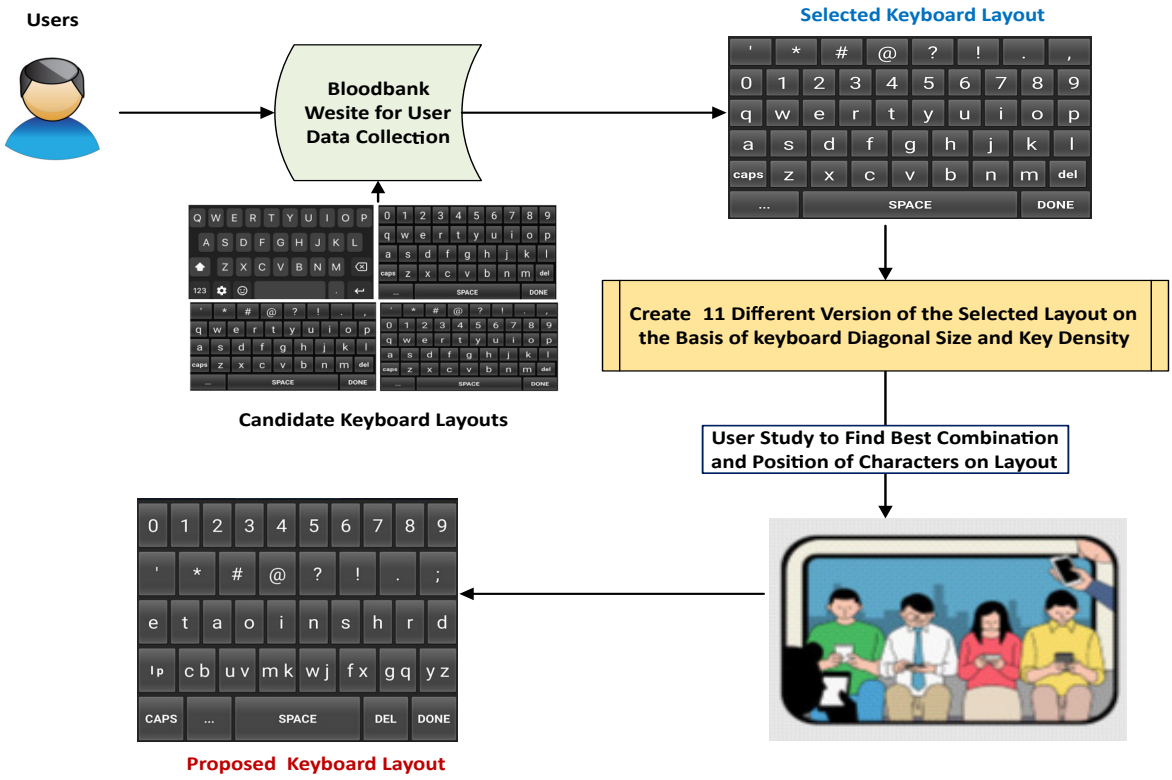

Figure 1. Approach Overview

slower typing speeds in comparison with traditional devices [13]. This work implies that putting a special character or digits in between the letters takes more effort on the smartphone than on the computer. This is due to the input constraint interface of the smartphone which has limitations in the size. Users need to change the pages of the keyboard to get access to a special character which creates frustration and eventually leads to the formulation of a weak password.

There are many factors that are the reason for the textual passwords generated from the smartphone becoming weaker [9]. A few existing works focused on increasing the typing speed on a smartphone keyboard layout. For instance, adding an extra chord on numeric feature phone [14–16].

Pressure-based text entry is also proposed for smartphones [17, 18] which has drawbacks like error-proneness.

The technological development has changed the landscape of the security systems. Smartphones are getting cheaper and cheaper with plenty of innovative features. People are not only using smartphones for calling and texting but also for email, web surfing and banking [19].

But due to the limitation of the keyboard size and the effort required to navigate between the pages password entry on smartphones is time-consuming and error-prone [7, 8, 20, 21]. This affects the usability and the strength of the textual passwords generated from the smartphones [22–24]. Despite these efforts, the creation of strong textual passwords from smartphones keeping the usability of the entry method remains one of the important research areas.

4. Methodology

In this work, a novel virtual keyboard configuration for the smartphone is proposed to minimize user typing error, and thereby enhance password creation ease and security. Figure 1 shows a high-level overview of the steps followed in our approach.

At first user data (keyboard interaction) is collected through a website developed by us. Users are presented with 4 different types of keyboard layouts while accessing from mobile devices. Among these, the one incurring fewer errors is chosen for further analysis. Then, 11 different version of the selected layout is created as candidate layouts with varying key sizes and character grouping per key. Extensive user studies are performed to explore the optimal configuration among these candidate layouts.

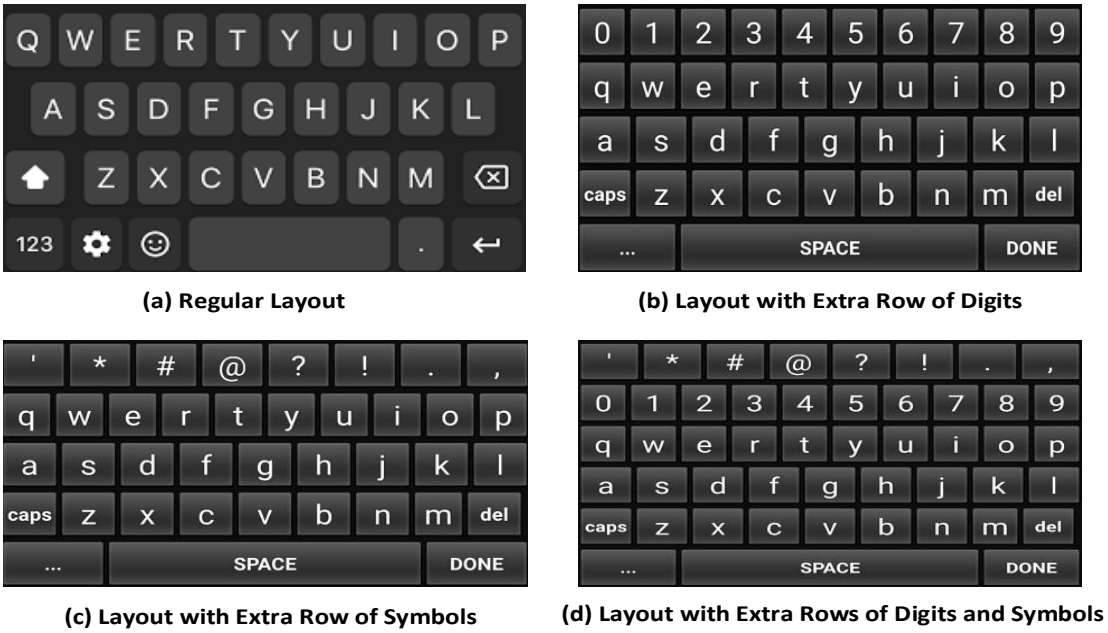

Figure 2. Keyboard Layout Options During User Registration Phase.

The following discussions detail these steps with experiment details and evaluation results.

4.1. User Survey 1: Analyze Four Standard Keyboard Layouts

4.1.1. User Demographics and Data Collection. The first step in our work is to record user interaction on smartphone virtual keyboards. For that, we developed a web application for a local blood bank that has more than 1,000 users. In the initial data collection phase, users accessed the website from many different types of devices. However, we only analyzed data entered through virtual keyboards on mobile devices.

We took caution in making sure that users' private data (name, date of birth, passwords, blood group, blood donation history, address, contact information, etc.) are not stored anywhere in plain text form. Any such data is encrypted and our data analysis tools only have the summary/statistics of characters/symbols entered by the user. We duly notified this information to the users and took proper consent for data analysis done as part of this work.

We collected user activity for three months. To assess user convenience, the web registration page also showed an option to choose between 4(four) keyboard layouts (Figure. 2) they will be using while using this app/website. A user's choice is saved and every time he/she logs in the chosen keyboard layout is used instead of the default. The 4 candidate layouts are chosen based on the following criteria: Regular Smartphone Keyboard Layout, With Extra Row of Digits, With Extra Row of Symbols and Keyboard Layout With Two Extra Rows of Symbols and Digits. It is to be noted that, the first three layouts shown in Figure. 2(a-c) are all standard layouts used in Android and iOS mobile operating systems and the literature [25–28]. Among them, the regular layout represents the default organization of keyboard characters found off the shelf in popular mobile operating systems, which is selected if the user does not choose otherwise.

Here, we have added the fourth one (Figure. 2(d)), which is a custom layout having two dedicated rows of digits and symbols. We know that every strong passwords often have the requirement of having at least one numeric character and a special character. Our intuition behind the design of this custom layout was that, how users react given the layout where these character options are presented in dedicated location in the soft keyboard.

Using these layouts, we collected information over a period of three months until at least 50 users' data were recorded per each configuration. To aid this process, during the registration process, users were prompted to select one of these 4 virtual keyboard layouts to enter their information (user-

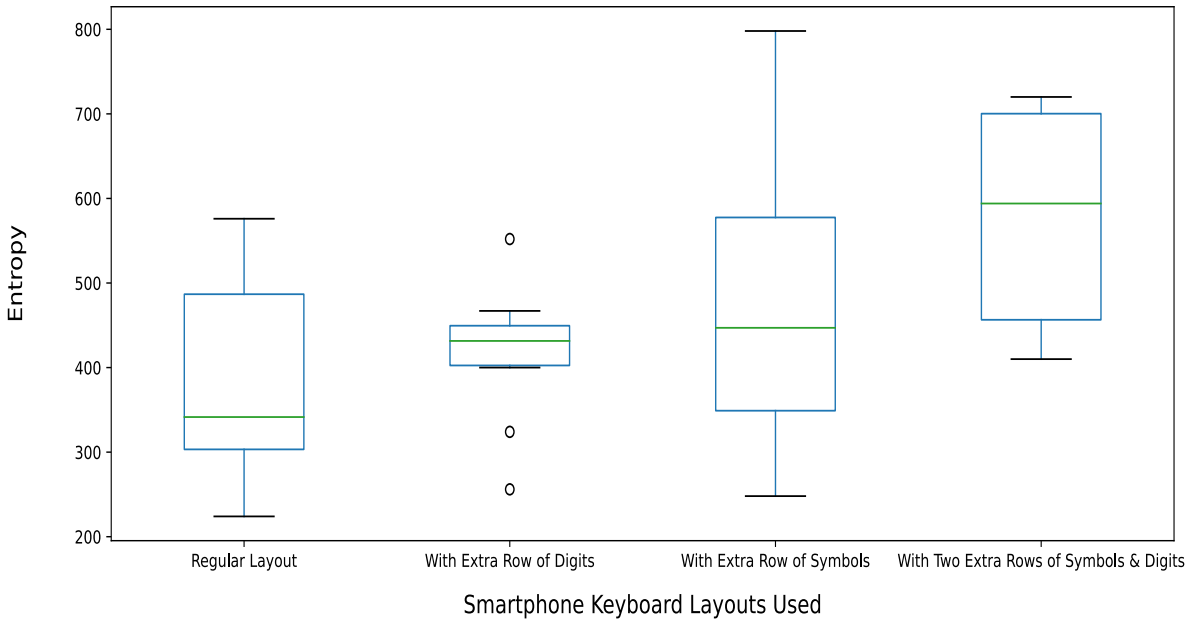

Figure 3. Entropy in Different Keyboard Layouts.

specific data and passwords). With the collected data, we perform error analysis and statistical analysis for the strength measurement of user-created passwords.

4.1.2. Performance and Usability Analysis. After that, we analyzed the collected data and ranked the layouts in terms of the strength of the created passwords and errors made by users in case of choosing and typing their passwords. Each backspace character pressed is regarded as one count of error.

At first, we evaluate the strength of the passwords created using those 4 layouts during the data collection phase. For that, we at first performed the entropy test.

Password entropy is based on the character set used to create a password. It predicts how difficult a given password would be to crack through guessing, brute force cracking, dictionary attacks or other common methods. Here, we have calculated the entropy value using Shannon entropy.

$$Entropy, E = L * log_2 N$$

where L is the length of the password and N is the size of the character. The character size is the sum of the sizes of different character types, Specifically: 26 lowercase letters, 26 uppercase letters, 10 digit characters and 92 symbols. The calculated entropy is shown in Figure. 3. It is evident from the entropy analysis that adding extra rows for digits and symbols encourages users to create stronger passwords.

From the box plot in Figure. 3, it is clear that the distribution of entropy of all layout are not similar. As mean is very sensitive to the extreme value, we analyze the entropy using variance comparison. One of the powerful variance analysis is one-way analysis of variance known as ANOVA test.

Analysis of Variance (ANOVA) test is a statistical method used to test differences between two or more means of data sets. Because this statistical method has ability to find the effect of outliers. It stands for ”Analysis of Variance” rather than ”Analysis of Means.” inferences on the statistical data are made by analyzing variance. This validates the statistical significance of data. From ANOVA test we found that the means were significant at 1% level. Which means that the password sets of different layouts have not similar strength. Now, to find which layout is superior in creating stronger password, we used LSD (least significant difference) test.

The least significant difference (LSD) test is used to identify the populations (sample) whose means are statistically different. The basic idea of the test is to compare the samples taken in pairs. It is then used to proceed in a one-way or two-way analysis of variance, given that the null hypothesis has already been rejected.

We made a mean comparison table (Table.1) to compare the original or sample means with LSD means. Here LSD1 stand for 1% significance and LSD5 means 5% significance from the above LSD test. For, the brevity of representations the follow-

Table 1. User Performance on 4 Primary Keyboard Layouts

Comparison of Sample Mean and LSD Means in Using Different Layouts			
Keyboard Layout Types	Sample or Original Mean	LSD Mean at 1% significance(LSD1)	LSD Mean at 5% significance(LSD5)
Smartphone Layout With Extra Two Rows of Symbols and Digits (SPSD)	81.25	65.24	69.39
Smartphone Layout With Extra Row of Symbols (SPS)	66.39	50.38	54.53
Smartphone Layout With Extra Row of Digits (SPD)	54.10	38.09	42.24
Regular Layout (SP)	48.34	22.33	36.48

Table 2. User Typing Speed Comparison in 4 Candidate Layouts

Layout Type	Typing Speed (characters/minute)
Regular Smartphone Layout	8
Layout with Extra Row of Symbols	56
Layout with Extra Row of Digits	61
Layout with Extra Row of Digits & Symbols	73

ing notations are used to represent the 4 candidate layouts in the Table.1. *SP* stands for Smartphone Regular Layout, whereas *SPS* and *SPD* denotes the layouts with dedicated rows of symbols and digits respectively.Finally, the custom layout created for this work with extra rows of digits and symbols are shown as *SPSD*.

As expected, the keyboard layout with two additional rows of symbols and digits came out as the clear winner. It has dedicated rows of digits and symbols which allowed users to type in their password without switching the page in most cases.

From Table. 1, we can make the following observations. As the LSD mean at 1% significance (LSD1) of SPSD layout(Highlighted) is less than the sample or original mean of SPS layout(Highlighted), so we found they behave similar in terms of password strength. But the LSD mean at 5% significance (LSD5) of SPSD layout(Highlighted) is greater than the sample or original mean of SPS layout, so we found the SPSD is better than SPS for password strength.

Next, we investigate how the typing speed(characters entry per minute) varies for different current layouts. The means of typing speed of survey participants using different layout has been pointed in Figure. 2.

It shows that adding an extra row of symbols or digits increases the typing speed of the textual passwords generated from the smartphone. The typing speed increases even more when two extra row of digits and symbols are added in the regular layout of the smartphone.This emphasizes the fact that extra row of symbols and digits reduce the time of changing the layer of keyboard for accessing digits and symbols which are generally not accessible from the first layer.

Hence, it is clear that it better to use two extra row of digits and symbols in virtual keyboard layout in smartphone. But there remain a question of usability. Also the size of layout should not be so large that users feel uncomfortable. For that, we perform the second user survey whose details are described next.

4.2. User Survey 2: Analyze Candidate Layout Design with Extra Rows of Digits and Symbols

The initial survey on user activities involving four different keyboard layouts showed that textual passwords generated from smartphones can be more strong and usable (less error-prone) while extra rows of symbols and digits are added. However, smartphones are input-constrained devices due to the limitation of the screen size, hence, there is an additional concern when the keyboard size is increased (adding extra rows of characters). For this reason, here we experimentally explore a key density range that will allow us to increase the soft keyboard size while keeping it usable (no loss of functionality or increase in typing errors).

The selected layout (Figure. 2(d))from the preliminary survey positioned the most used symbols in the first row, digits in the second row, and regular alphabet characters next. However, this arrangement was done naively as a starting point. To find the optimal arrangement, we created 11(eleven) separate keyboard layouts by rearranging the key positions and grouping on soft buttons, changing key sizes within a standard dimension size. The details of

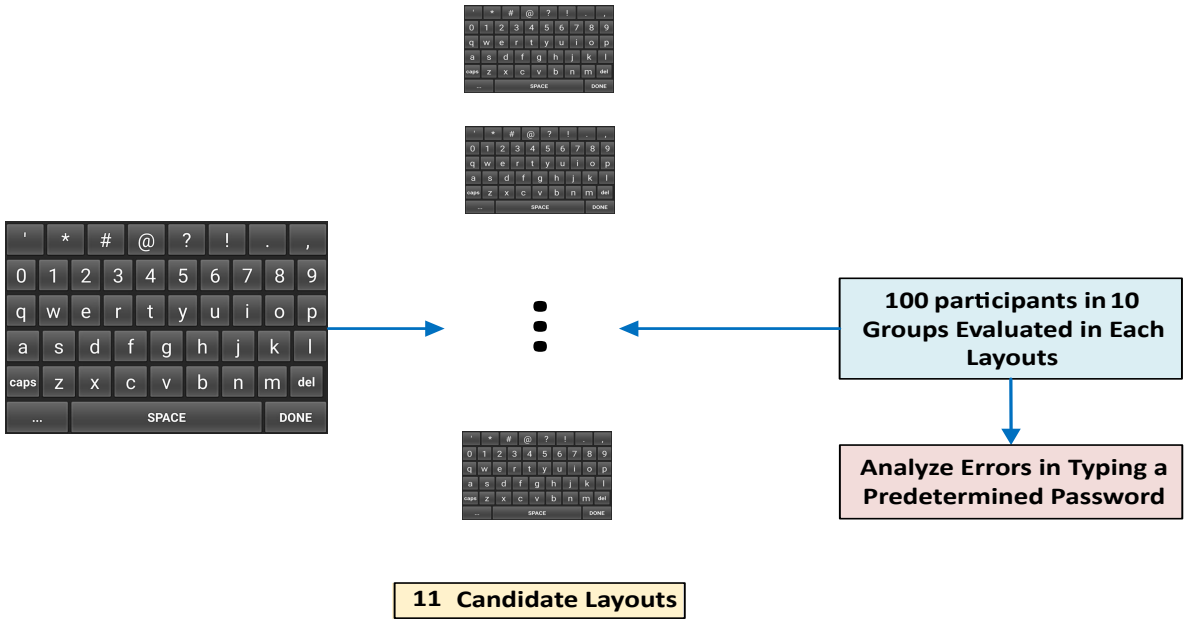

Figure 4. User Experiment Steps on 11 Candidate Layouts in 2nd Survey

these layout designs and user experiments are described below.

For this, we varied keyboard dimensions, the number of keys in each soft button, the number of switches required to access all digits, symbols, and letters, etc. User thumb size also plays an important role in designing these configurations. Researchers [29–31] find that for maximum user comfort, the diagonal distance of a smartphone virtual keyboard should be around 75% of the user's thumb size. It is also observed that a comfortable range of key sizes on a smartphone soft keyboard ranges from 20 dP(density pixel) to 70 dP.

To design the candidate layout configurations with different key densities and diagonal lengths we made sure that these factors were maintained. In the next section, we present the findings of the user study on these 11 candidate layouts to find out the optimal arrangement.

Here, we describe the details of the user survey on 11 candidate layouts, designed as part of this study. All of the layouts are evaluated using 10 different user groups of various demographics and educational backgrounds. Here, each group contains 10 participants. So, in this phase, 100 user data were collected and analyzed to find the best configuration. This user experiment process is highlighted in Figure. 4. The following discussion describes this experiment and the findings in detail.

4.2.1. Environment Setup. For the experiment, we chose a Samsung Galaxy J8 smartphone running Android 9.0 (Pie) and having a screen size of 6 inches. Most modern smartphone screens are between 5.5 and 6 inches [32]. So, the selected screen size gives us a good balance in that regard.

4.2.2. Demographic of Participants. As mentioned above, this phase of the user survey was done on 100 participants who were split into 10 groups having 10 participants per group. Participants were recruited from the pool of users registered on our blood bank website. We took caution that, they include (not necessarily in equal portion but not making the distribution imbalanced either) people from different profession and educational backgrounds where the male female ratio was 60:40. The demographics of survey participants are listed in Table . Among them, the participants of 10 user groups are chosen randomly.

Table 4. Demographic of Survey Participants

Profession	Number of Participant
University Students	24
Doctors	15
Military Personnel	14
Government Employees	18
Engineers	17
Business Person	12
Total	100

4.2.3. Evaluation and Findings. Users were asked to enter a system-generated random password using

Table 3. User Experiment Result on 11 Candidate Layout (Key Size and Density vs Error Rate)

Key size (DP)	Density ($keys/cm^2$)	Diagonal Length (cm)	Avg. Error Rate
20	2.32	7.4	11.15%
25	1.92	7.58	10%
30	1.59	7.82	9.3%
35	1.39	8.06	5.8%
40	1.21	8.38	4.6%
45	1.07	8.72	2%
50	0.97	9.02	0%
55	0.88	9.41	3%
60	0.80	9.83	13.83%
65	0.75	10.18	20%
70	0.69	10.63	30%

a given layout from the pool of candidate configurations. All 10 participants from the same group were given the same layout configuration. Our system then records the number of errors (no of backspace characters) and the keystroke duration of the users. This process is repeated for all the 11 candidate configurations with 10 users per layout.

Table 3 lists the findings of this study. Each row reports the particular configuration setting along with the mean error averaged over the 10 users per layout. The results show that the key sizes in the range of 40 to 55-pixel density result in the least average error and within the tolerable range (less than 5%). Based on that, the optimal key density appears to be in the range of 0.88 to 1.21 $keys/cm^2$. Similarly, we also get a good idea of what the keyboard diagonal length should be between 8.38 and 9.41 cm.

Apart from that, we also analyze the keystroke duration of the participants. Due to the limitation of the smartphone keyboard size, the time of stroking a key varies in different layouts of smartphones.

As shown in Figure. 5, for the diagonal of the keyboard layouts from 7.4 cm to 9 cm, we see that the average time for keystroke remains unchanged. When the diagonal of the keyboard increases from 9 the average time of keystroke increases due to the limitation of the human thumb size.

So, from our experiments, we could get a fair estimate of key densities, keyboard diagonal size, and key size in pixel density for a smartphone virtual keyboard with dedicated rows for digits and commonly used symbols. From these measurements, we can say that the addition of extra rows of symbols and digits will not reduce the usability of the keyboard until the key density and the diagonal range are between the above-mentioned range.

5. Threats to Validity

We made an effort to ensure a fair and representative allocation of survey respondents for each step of this multi-step study. We do, however, accept that despite our best efforts, we were unable to expand the survey's participant pool, and as a result, we may have missed a number of data points.

This work also does not delve into details of password security mechanisms or how to improve password-based authentication. For the same reason, this paper does not cover other authentication schemes such as biometrics and multi-factor authentication.

Our work is specifically designed with the goal of finding what should be the optimal layout configuration in case we allocate dedicated rows for digits and special characters. Here, this scenario is the starting point in candidate layout design. However, here we are not attempting to show the proposed layout as a generalized or standard layout. A good keyboard layout configuration can be different from the one proposed here. Rather, the proposed system investigates two of the requirements of strong passwords - the presence of numeric and special characters and the studied layouts see how this requirement can be facilitated with its design. Other requirements for strong passwords such as lowercase and uppercase letter combinations, password length, and user-specific choices are out of the scope of this work.

This is also to be noted that, the four initial layouts we evaluated are from the Android operating system with the last one being customized. We did not evaluate our method in the iOS environment. However, the proposals made are agnostic of the platform and can be adapted to other systems without much modifications.

The nonstandard layouts which may be certain applications specific and often appear in case of very

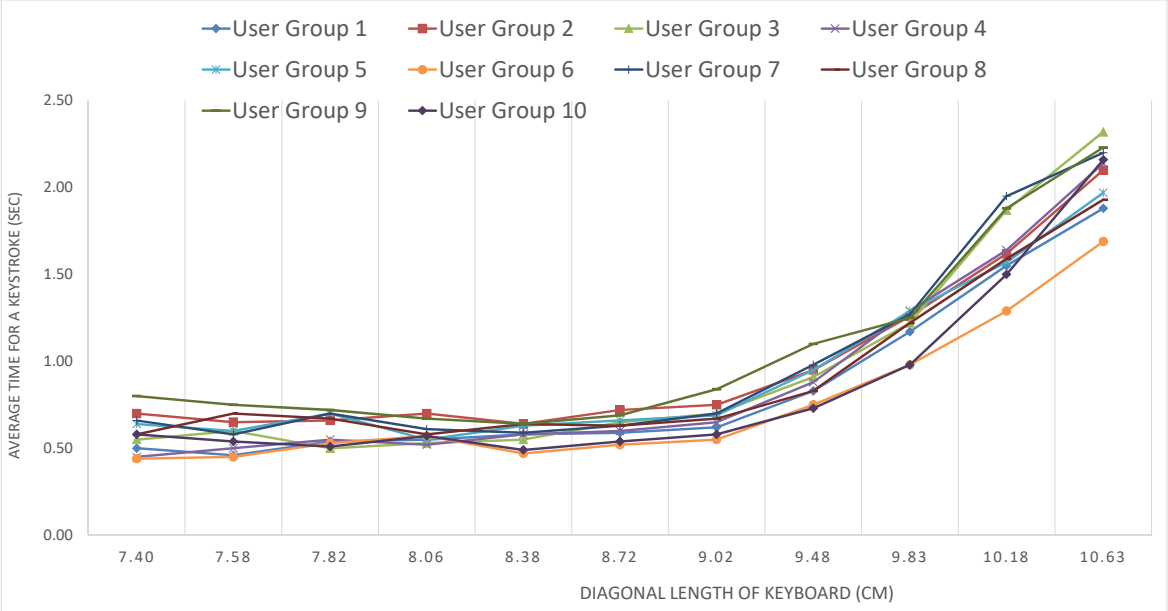

Figure 5. Dependency of Keystroke Time on the Diagonal Length of the Keyboard

small screen sizes are also not investigated. Here, we focused on how the dedicated rows of digits and special characters can motivate the password creation behavior of the standard layout users. In the case of nonstandard layouts, even for very simple passwords users need to make a lot of keyboard face switches compared to standard layouts, so of out of consideration here.

Given these limitations, we acknowledge that the outcomes of our study might have missed some important observations along with the corresponding approaches to address them.

6. Conclusion

In conclusion, this thesis has explored the critical issue of smartphone keyboard layout configuration and its potential to aid in the creation of stronger passwords. As we live in an increasingly digitized world, the importance of robust password security cannot be overstated. Passwords are the primary means of safeguarding sensitive information, and their strength is paramount in protecting individuals and organizations from various cyber threats.

Our research found that smartphone keyboards can be expanded with dedicated rows for special character groups such as digits and symbols without sacrificing usability or security. It was also observed that, virtual keyboard layout with two dedicated rows of digits and symbols, the optimal key density should be between 0.88 to 1.21 $keys/cm^2$. For the same scenario, the keyboard diagonal length should be between 8.38 and 9.41 cm.

This work investigated the impact of smartphone keyboard layout design in encouraging users to create stronger passwords. By considering both security and usability, designers can contribute to the overall cybersecurity landscape. As technology evolves, the importance of password security remains constant, and research in this field will continue to be vital in adapting to emerging challenges and threats. Ultimately, the findings presented in this thesis offer valuable insights into a practical approach to enhancing password security on mobile devices, contributing to a safer and more secure digital environment for all.

In the future, we would like to extend our work to accommodate the following aspects of the proposed system. At first, we plan to evaluate our system on other popular smartphone operating systems such as iOS. To further ensure the proposed layouts serve the envisioned purpose, further user studies will be required to be performed on various nonstandard smart screens and layout configurations. Finally, we need to evaluate the system with more users to validate and make necessary modifications to the proposed system. We believe that our system can help future designers take the proposed idea and enhance on top of it to come up with usable yet effective smartphone keyboard layouts

References

[1] M. M. Baig and W. Mahmood, "A robust technique of anti key-logging using key-logging mechanism," in *2007 Inaugural IEEE-IES Digital EcoSystems and Technologies Conference*. IEEE, 2007, pp. 314–318.

[2] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Information and Software Technology*, vol. 94, pp. 30–37, 2018.

[3] K. Fujita and Y. Hirakawa, "A study of password authentication method against observing attacks," in *2008 6th International Symposium on Intelligent Systems and Informatics*. IEEE, 2008, pp. 1–6.

[4] D. Dasgupta, A. Roy, A. Nag *et al.*, *Advances in user authentication*. Springer, 2017.

[5] C. Herley, P. C. Van Oorschot, and A. S. Patrick, "Passwords: If we're so smart, why are we still using them?" in *Financial Cryptography and Data Security: 13th International Conference, FC 2009, Accra Beach, Barbados, February 23-26, 2009. Revised Selected Papers 13*. Springer, 2009, pp. 230–237.

[6] T. I. Tanni, T. Taharat, M. S. Parvez, S. T. A. Rumee, and M. I. Zaber, "Is my password strong enough?: A study on user perception in the developing world," *EAI Endorsed Transactions on Creative Technologies*, vol. 9, no. 30, 2 2022.

[7] T. Matthews, J. Pierce, and J. Tang, "No smart phone is an island: The impact of places, situations, and other devices on smart phone use," *IBM RJ10452*, pp. 1–10, 2009.

[8] M. Jakobsson and R. Akavipat, "Rethinking passwords to adapt to constrained keyboards," *Proc. IEEE MoST*, pp. 1–11, 2012.

[9] S. Haque, M. Wright, and S. Scielzo, "Passwords and interfaces: towards creating stronger passwords by using mobile phone handsets," in *Proceedings of the Third ACM workshop on Security and privacy in smartphones & mobile devices*. ACM, 2013, pp. 105–110.

[10] Y. Yang, J. Lindqvist, and A. Oulasvirta, "Text entry method affects password security," in *The {LASER} Workshop: Learning from Authoritative Security Experiment Results ({LASER} 2014)*, 2014.

[11] S. Gupta, A. Buriro, B. Crispo *et al.*, "Demystifying authentication concepts in smartphones: Ways and types to secure access," *Mobile Information Systems*, vol. 2018, 2018.

[12] R. Susik and S. Grabowski, "Keydrop: Dynamic keyboard layout for faster typing and fewer typos," *International Journal of Human–Computer Interaction*, pp. 1–9, 2023.

[13] P. Bao, J. Pierce, S. Whittaker, and S. Zhai, "Smart phone use by non-mobile business users," in *Proceedings of the 13th international conference on human computer interaction with mobile devices and services*. ACM, 2011, pp. 445–454.

[14] N. Patel, J. Clawson, and T. Starner, "A model of two-thumb chording on a phone keypad," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2009, p. 8.

[15] J. O. Wobbrock, B. A. Myers, and H. H. Aung, "The performance of hand postures in front-and back-of-device interaction for mobile computing," *International Journal of Human-Computer Studies*, vol. 66, no. 12, pp. 857–875, 2008.

[16] D. Wigdor and R. Balakrishnan, "A comparison of consecutive and concurrent input text entry techniques for mobile phones," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2004, pp. 81–88.

[17] S. A. Brewster and M. Hughes, "Pressure-based text entry for mobile devices," in *Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services*. ACM, 2009, p. 9.

[18] G. Tai, D. Wei, M. Su, P. Li, L. Xie, and J. Yang, "Force-sensitive interface engineering in flexible pressure sensors: A review," *Sensors*, vol. 22, no. 7, p. 2652, 2022.

[19] A. P. Felt and D. Wagner, *Phishing on mobile devices*. na, 2011.

[20] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," in *Proceedings of the 11th international conference on mobile and ubiquitous multimedia*. ACM, 2012, p. 13.

[21] J. Chang and K. Jung, "Effects of button width, height, and location on a soft keyboard: task completion time, error rate, and satisfaction in two-thumb text entry on smartphone," *IEEE Access*, vol. 7, pp. 69 848–69 857, 2019.

[22] E. Von Zezschwitz, P. Dunphy, and A. De Luca, "Patterns in the wild: a field study of the usability of pattern and pin-based authentication on mobile devices," in *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services*. ACM, 2013, pp. 261–270.

[23] L. Mecke, D. Buschek, M. Kiermeier,

S. Prange, and F. Alt, "Exploring intentional behaviour modifications for password typing on mobile touchscreen devices," in *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, 2019, pp. 303–317.

[24] Y. Li, Y. Cheng, W. Meng, Y. Li, and R. H. Deng, "Designing leakage-resilient password entry on head-mounted smart wearable glass devices," *IEEE Transactions on Information Forensics and security*, vol. 16, pp. 307–321, 2020.

[25] Y. Korkmaz and P. O. Durdu, "Comparison of user performance and satisfaction of tablet virtual keyboards in three different os environment," in *2015 9th International Conference on Application of Information and Communication Technologies (AICT)*. IEEE, 2015, pp. 269–273.

[26] A. Gkoumas, A. Komninos, and J. Garofalakis, "Usability of visibly adaptive smartphone keyboard layouts," in *Proceedings of the 20th Pan-Hellenic Conference on Informatics*, 2016, pp. 1–6.

[27] K. K. Greene, M. A. Gallagher, B. C. Stanton, and P. Y. Lee, "I can't type that! p@ w0rd entry on mobile devices," in *Human Aspects of Information Security, Privacy, and Trust: Second International Conference, HAS 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 2*. Springer, 2014, pp. 160–171.

[28] P. Y. Bagaskara, M. A. Muhammad, M. Komarudin *et al.*, "Virtual keyboard design of lampung script based on android," *International Journal of Electronics and Communications System*, vol. 2, no. 1, 2022.

[29] J.-M. Cha, E. Choi, and J. Lim, "Virtual sliding qwerty: A new text entry method for smartwatches using tap-n-drag," *Applied ergonomics*, vol. 51, pp. 263–272, 2015.

[30] P. Parhi, A. K. Karlson, and B. B. Bederson, "Target size study for one-handed thumb use on small touchscreen devices," in *Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, 2006, pp. 203–210.

[31] Y. S. Park and S. H. Han, "Touch key design for one-handed thumb interaction with a mobile phone: Effects of touch key size and touch key location," *International journal of industrial ergonomics*, vol. 40, no. 1, pp. 68–76, 2010.

[32] Y. Li, F. You, M. Ji, R. J. Zhang, and X. You, "Effect of gestures and smartphone sizes on user experience of text input methods," *Universal Access in the Information Society*, pp. 1–18, 2022.