

A New User-Apps Interactions Dataset for Behavioral Profiling Using Smartphones

Saud Alotaibi¹, Abdulrahman Alruban^{1,2}, Moneerah Alotaibi^{1,3}, Ali Alshumrani^{1,4}
Abdulaziz Altamimi¹

¹Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK

²Computer Sciences and Information Technology College, Majmaah University, Al Majma'ah, Saudi Arabia

³Computer Science Department, Shaqra University, Shaqra, Saudi Arabia

⁴ College of Computers and Information Systems, Umm Al-Qura University

Abstract

The use of mobile devices in our daily lives has grown steadily. These mobile devices contain sensitive data such as text messages, photos, communication logs, contact lists, personal information and stored passwords. They are also used to perform activities such as sending emails or transferring money via mobile Internet banking, which is considered a sensitive process. As a consequence, more security is needed on mobile devices since, after point-of-entry authentication, the user can perform almost all tasks without having to re-authenticate. On the other hand, many authentication methods have been suggested to improve the security of mobile devices in a transparent and continuous manner, providing a basis for convenient and secure user re-authentication. In addition, although a number of studies have investigated the feasibility of using behavioural biometrics to secure a mobile device, there is a lack of studying user behavioural profiling interactions with their smartphones due to there are no such datasets available. The main aim of this paper is to present a new user-apps Interactions dataset for behavioral profiling using Smartphones which might help researchers to improve smartphones security. A study involving data collected from 76 users over a 1-month period was conducted, generating over 3 million actions based on users' interactions with their smartphone. This study also demonstrates and highlights some future work by utilizing the acquired dataset to provide robust, continuous and transparent authentication and usable system as well.

1. Introduction

The use of mobile devices in our daily lives has grown steadily, due to the combination of mobility and 24/7 multi-connectivity. In particular, smartphones are used to perform activities, such as sending emails, transferring money via mobile Internet banking, making calls, texting, surfing the Internet, viewing documents, storing medical, confidential and personal information, shopping

online and playing games. As a result, mobile devices have overtaken desktop computers. For instance, the total number of smartphone users worldwide from 2014 to projections for 2022 [1]. In addition, the number of smartphone users in 2019 is forecast to pass 5 billion. For example, in the USA, the number is forecast to grow to 247.5 million by 2019 [1]. Globally, there are 3.419 billion people connected to the Internet (equating to 46% global penetration), while 2.307 billion users are actively involved in social media. In addition, 3.790 billion people are unique mobile users (representing 51% global penetration), whereas 1.968 billion users utilise social media on a mobile device [2].

Statista [2] predicted that, in 2020, the expected growth of mobile app revenue would be \$101 billion, from \$41.1 billion in 2015. It was expected that revenue from mobile apps would grow at a steady rate in the coming years. Moreover, mobile web traffic was expected to exceed 10 exabyte by 2017 [3]. Regarding the digital marketing review [4], mobile devices achieve 75% of all adults' time online with smartphones. On the other hand, 80% of female spend their time on mobile devices compare with only 69% for males and 30% of online adults are now mobile only as well. Based on audience, over 90% of time online is spent on smartphones for Spotify and Snapchat whereas tablets account for over a third of time spent on the BBC as illustrated in Figure 2 2. In addition, YouTube increased both its mobile app audience (about 5%) and time spent (about 22%) compared to 2017. Interestingly, Snap is the only mobile app in the top 10 which is not owned by Google or Facebook. Furthermore, Spotify, Netflix and eBay feature in the top 10 mobile apps for time spent [4].

Currently, sensitive data such as text messages, contact lists, and personal information are stored on mobile devices. This makes authentication of paramount importance. More security is needed on mobile devices since, after point-of-entry authentication, the user can perform almost all tasks without having to re-authenticate. [5, 6]. As a result, there is an urgent need to verify the identity of the current user of a mobile device. It must be possible to authenticate legitimate users and detect imposters in a continuous and transparent manner, maintained

beyond point-of-entry, without the explicit involvement of the user [7]. To this end, data on user behaviour is gathered in the background without requiring any dedicated activity by the user, by regularly and periodically checking user behaviour in order to continuously monitor the protection of the mobile device [8]. In addition, although a number of studies have investigated the feasibility of using behavioural biometrics to secure a mobile device, there is a lack of user action interactions with their smartphones dataset to investigate the behavioural

profiling, as shown in Table 1. This research study considered this and collected a total of 3,015,339 actions which might be helpful for the researchers.

The next section presents related work and the state of the art of smartphone behaviour profiling biometrics. This is followed by an outline of a data collection methodology to smartphone security in section 3. Then, section 4 presents data collection analysis with more explanations and discussions. Finally, section 5 concludes the paper.

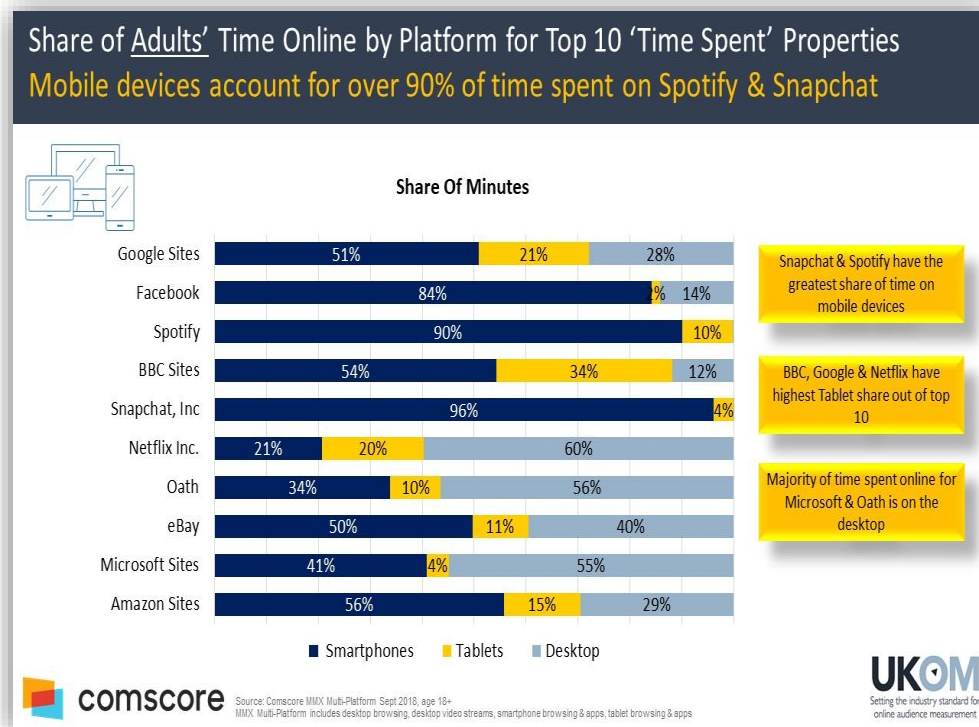


Figure 1. UK digital marketing review [4]

2. Related Work

It is commonly acknowledged that biometric authentication is a reliable solution to authenticating users using convenient and trusted methods [9, 10]. Most biometric authentication systems are capable of providing a wide range of transparent authentication approaches to achieve a high level of balance between usability and security [6]. In this context, behavioural biometrics is often presented as a suitable authentication method and, indeed, is commonly used for transparent and continuous authentication while ensuring usability [5, 11]. One type of behavioural biometric is behaviour profiling. The main aim in this case is the transparent verification of mobile users based on the way they interact with the required service whilst using their smartphone [5,12]. This approach compares the current user's activities with a

historical profile of usage that is built utilising a machine learning method [13].

Although a limited number of studies have focused on behavioural profiling-based authentication for mobile devices, some investigative efforts have been made in the literature to introduce behavioural profiling as a behavioural biometrics authentication approach to providing transparent authentication [6]. For instance, Li et al. [14] introduced a behaviour profiling approach to identify mobile device misuse by focusing on the mobile user's application usage. This work used the MIT Reality Mining dataset [15]. The following data were collected from 100 smartphone users for 9 months: application information (app name, date, duration of usage and cell ID), voice call data (including date, time, number called, duration, and cell ID), and text message data (date, time, number texted and cell

ID) [12, 13]. Later, the authors presented a novel behaviour profiling framework that was able to collect user behaviour to evaluate the system security status of a device in a continuous manner before sensitive services were accessed [16]. They investigated the sensitivity of the application concept, which is mapped to high-risk levels to make the framework more secure and transparent when the user requires access to high-risk applications. The authors concluded that the approach seems able to distinguish mobile users through their application usage; in particular, by focusing on the names of applications and the location of usage, which are considered valuable features.

Among further studies in a similar context, Saevanee et al. [17] examined the combination of three diverse biometric methods: keystroke dynamics, behavioural profiling and linguistic profiling from 30 virtual users (the dataset was not real and was gathered from different datasets). To continue their work, Saevanee et al. [18] presented a text-based authentication framework utilising the above modalities and introduced a security aspect by allowing the user to set security levels for access to different applications. In other recent work, Fridman et al. [19] proposed a parallel binary decision-level fusion architecture for active authentication. The fusion is used for classifiers based on four biometric modalities: text analysis,

application usage patterns, web browsing behaviour, and the physical location of the device through GPS (outdoors) or Wi-Fi (indoors). To evaluate the framework, the authors collected a dataset from 200 users' Android mobile devices over a period of 5 months.

In the same context, Neal and Woodard [20] introduced associative classification to authenticate mobile device users by analyzing the performance of applications. Bluetooth and Wi-Fi data were collected from 189 college-level students over 19 months. Three time intervals (5, 15, and 30 min) were selected and association rules were extracted from each data type separately and combined as features. Prior to that, Shi et al. [21] recorded users' routines, such as location, phone calls, and application usage, in order to build a profile and assign a positive (e.g., good behaviour, such as a phone call to a known number) or negative score for each user's routine, using a dataset based on 50 users for a period of 12 days or more. The dataset contained SMS, phone call, browser history and location, without demonstrating the finding of this study.

To conclude, there is a lack of user action interactions with their smartphones dataset to investigate the behavioural profiling, as shown in Table 1.

Table 1. Datasets results

Study	# of Subject	Dataset	Features
Shi et al. , (2011) [21]	50 for	12 days	SMS, Calls, Browser History,GPS
Hayashi et al. , (2012) [23]	20	Structured interview	-
Gupta et al., (2012) [24]	37–76	MIT Reality	GPS location, WIFI, Bluetooth
Li et al., (2014) [16]	22–76	MIT Reality	App name, Tel. number, cell, GPS
Khan and Heng., (2014)[22]	30	4different datasets	-
Kayacik et al, (2014) [25]	7,35,100	GCU, MIT Reality	Wi-Fi, CPU load, light, noise
Fridman et al. (2015) [19]	200	30 days	Text , app usage, Wi-Fi, GPS
Neal and Woodard (2017) [20]	189	students	Bluetooth and Wi-Fi data
Acien et al .(2019) [26]	48	Maryland University	App usage, GPS, Wi-Fi, Touch

Note: n/a = not applicable

On the other hand, predicting mobile app usage has motivated researchers in the past, there are some research in this area. Tan et al. [28] conducted experiments on the Nokia MDC dataset that involves 38 users and proposed an algorithm to predict mobile application usage patterns. Huang et al. [29] discuss the faster execution of desired app through the pre-loading of the right apps in memory or through app pop up to the mobile's home screen. They exploit a set of feature such as time, location, and the user profile, to predict the user's app usage using the Nokia MDC dataset already mentioned. Yan et al. [30] developed app

preloading method that use contextual information such as user location and temporal access patterns to predict app launches with 34 users. Also, Zou et al. [31] developed some light-weighted Bayesian models that use the app usage history to predict the next app that user is going to use. Liao et al. [32] developed a widget that use temporal profiles which identify the relation between apps and their usage times in order to predict user's app usage. In addition, Pan et al. [33] used social information coming from friends of the user in a social networks to predict the most likely mobile application that a user will install. Krishnaswamy

et al. [34] developed a different prediction method that discovers frequent co-occurrence patterns on the phone to indicate to the context events that frequently occur together.

3. Mobile Data Collection Methodology

In order to investigate the feasibility of building a transparent and continuous biometric-based system, it is necessary to collect samples of genuine user interactions with their mobile devices/apps, based upon a substantive period of real-world use (noting that such samples would be based upon data that are naturally logged by apps on the devices already and so the research would not be gathering information that was not already available – it would, however, be applying it to an additional purpose). As such, it was proposed to enlist participants and collect log data from them after one month of normal device usage. It should be noted that the data were anonymous and that participation did not require the participants to do anything other than use their devices as normal. This experiment collected the sort of data that are logged routinely, such as a time stamp of the application used by the participant and the name of the user action (read, send, etc.) but did not collect data such as passwords or messages.

The experiment was carried out on the participants' Android mobile phone as shown in Figure 2. Ethical approval for this research project was obtained from the university's Research Ethics Committee in order to fulfil University of Plymouth requirements. All the participants were 18 years or older and were asked to read and sign a consent form and information sheet regarding data

collection before starting the experiment. In addition, the research and data were conducted and stored within the Centre for Security, Communications and Network Research (CSCAN) at Plymouth University (start date: February 2017; end date: July 2017). Although the study was conducted to collect app log data, no sensitive material was involved. To facilitate a meaningful analysis, at least 100 adult participants (18 years or older) were invited to participate in this metadata capture experiment. Participants took at least one month to complete their participation in the study, during which time they were simply asked to use their device as normal.

For the purpose of the data collection, a code was developed to extract log files from a backup file from the participants' devices after taking a backup after one month on the principal investigator. After one month, each participant's mobile device was connected to the main investigator's computer. Mobile backup was started by utilising Android Debug Bridge (ADB) [27], which is a command line tool that allows communication between the connected Android device and a computer. This necessitated the participating devices having Android OS version 4.1 or above. To access iOS, there is a need to jailbreak the devices to access the log files which unlikely for the users to accept that. On the other hand, android allow to access to mobile detailed and extract data log files without the need to root. In addition, to protect the user privacy, ADB was used instead of asking the mobile user to download application.

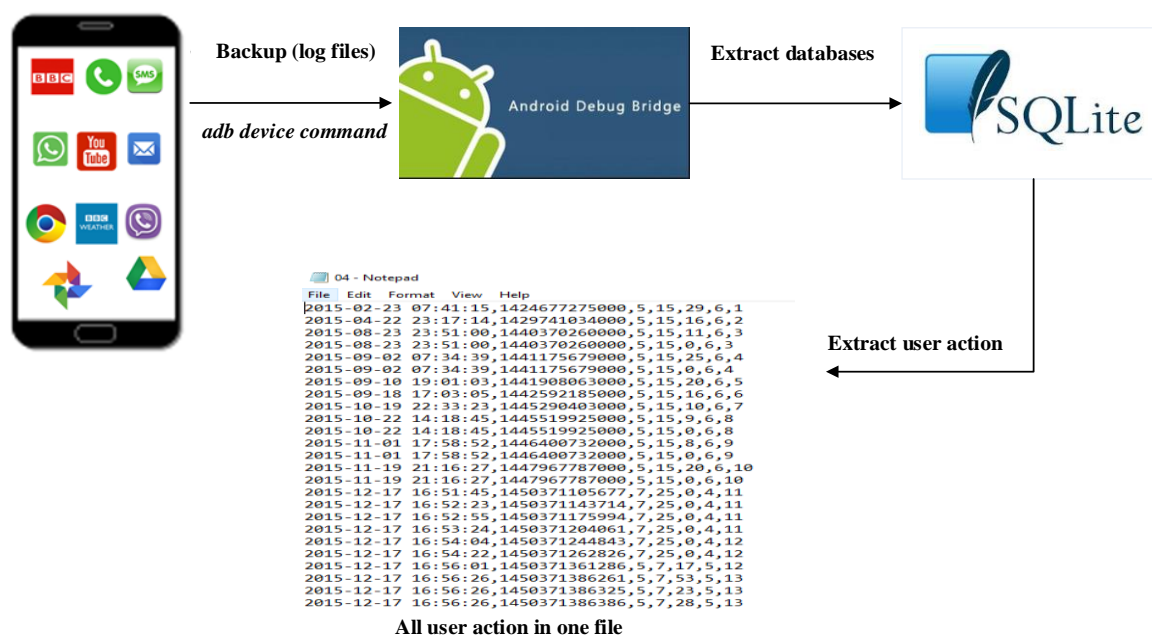


Figure 2. Data Collection Methodology

The backup file was extracted and the participant's mobile phone was disconnected. Then, a code was run on SQLite to extract the log files from the extracted backup file. Next, data were generated and the information column was exported to a datasheet file (the time stamp, application name and process name) and stored in a folder called the "UserActionDataSheet". The data were then reviewed by the participant to verify that he/she agreed to share them with the investigator. Finally, the backup file was removed at the end of the experiment period. Although the study is going to collect app log data, there is no sensitive material involved in doing this by writing a code to

extract all data automatically once connect the mobile device and protect the user privacy.

During this phase of the data collection, the following applications were selected and collected, as shown in Table 2, and a package name and database name given to each selected application. Some applications, such as Facebook, Online Mobile Banking, and Chrome, were fully encrypted and there was no way of collecting user data without compromising the user's privacy by asking the participant to root his/her device. For this reason, only 12 applications were collected in order to protect the user's privacy.

Table 2. Applications collected from users' mobile phones

App Name	Package name	Database name
Phone Call	om.sec.android.provider.logsprovider	logs
SMS	com.sec.android.provider.logsprovider	logs
Downloading	com.android.providers.downloads	downloads
YouTube	com.google.android.youtube	history
WhatsApp	com.whatsapp	msgstore
Browser	com.sec.android.app.sbrowser	SBrowser_Tabs
Google Play	com.android.vending	localappstate
Email	com.android.email	EmailProvider
Viber	com.viber.voip	viber_data; viber_messages
Google Photo	com.google.android.apps.photos	gphotos0_local_media
Camera	com.android.providers.media	external_Images
		external_video
Yahoo mail	com.yahoo.mobile.client.android.mail	mailsdk_messages

4. Mobile Dataset Analysis and Discussion

At the end of the data collection, the 76 users had completed the process and the analysis phase was ready to begin. Each user's data were stored in an individual text file, each record containing the following fields: the date (in two forms: human time and a timestamp e.g., 2016-06-28 20:22:30, 1467141750071), application name, action type, and extra information, such as message/email length and call duration. In this study, a total of

3,015,339 actions with total usage daily 22457 was accumulated where the long total usage day was 1230 days and 35 was the short total usage day. Table 2 demonstrate the outcomes of such real time behavioural data collection by summering a 47 user action were gathered from 12 applications of 76 participants as shown in Table 3. In this context, the long total usage day was 1230 days, and 35 was the short total usage day. This, in turn, means that the large dataset sample size might lead to a high degree of accuracy, which would have a positive impact on the conclusions drawn from the proposed approach.

Table 3. 47 User actions collected

No.	Application	Action	No.	Application	Action
1	Phone Call	Make a Call	25	Google Play	Download app
2	Phone Call	Receive a Call	26	Google Play	Update app
3	SMS	Read a SMS message	27	Email	Send an email
4	SMS	Send a SMS message	28	Email	Read an email
5	Downloading	Download a file	29	Viber	Make a free voice Call

No.	Application	Action	No.	Application	Action
6	YouTube	Search on YouTube	30	Viber	Make a video Call
7	WhatsApp	Receive a text message	31	Viber	Receive a voice Call
8	WhatsApp	Receive an image message	32	Viber	Receive a video Call
9	WhatsApp	Receive an audio message	33	Viber	Receive a text message
10	WhatsApp	Receive a video message	34	Viber	Receive an image message
11	WhatsApp	Receive a contact card	35	Viber	Receive a sound message
12	WhatsApp	Receive a location	36	Viber	Receive a location
13	WhatsApp	Receive a free call	37	Viber	Send a text message
14	WhatsApp	Receive a PDF file	38	Viber	Send an image message
15	WhatsApp	Send a text message	39	Viber	Send a sound message
16	WhatsApp	Send an image message	40	Viber	Send a location
17	WhatsApp	Send an audio message	41	Viber	Delete a message
18	WhatsApp	Send a video message	42	Google Photo	Upload an image
19	WhatsApp	Send a contact card	43	Google Photo	Upload a video
20	WhatsApp	Send a location	44	Camera	Take a photo
21	WhatsApp	Make a free call	45	Camera	record a Video
22	WhatsApp	Send a PDF file	46	Camera	Save a photo
23	Browser	Search	47	Camera	Save a Video
24	Browser	Watch a video			

In this section, the overview of the acquired dataset was presented. The histogram in Figure 3 highlights the differences that might be considered significant compared with the total population. For instance, the user profile for participant 71 can be differentiated from the others due to the mobile

phone mainly being used from 00:00 AM until 6:00 AM, whereas the majority of participants used their mobile phones from 8:00 AM to 10:00 PM. On the other hand, four participants (42, 47, 53, and 68) show identical usage compared with the population.

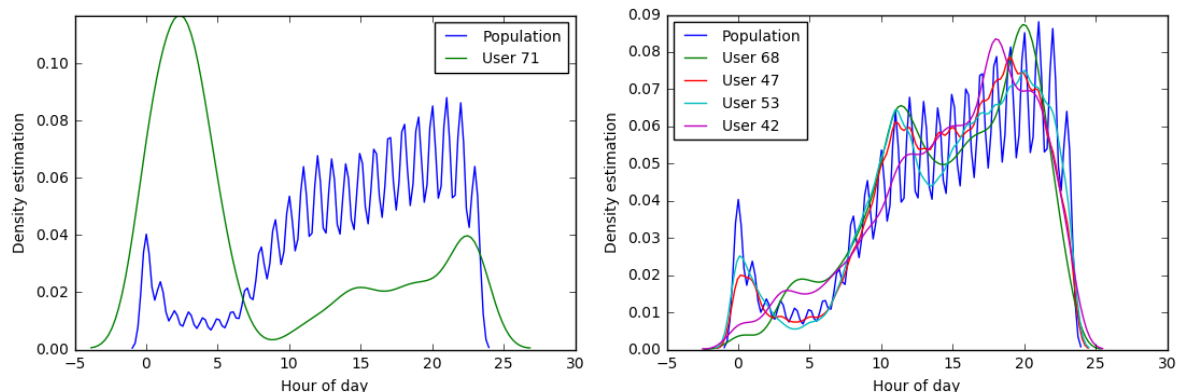


Figure3: Histogram for population compared with partipents

Figures 4 show that a different sample of behavioral profiling for different users. It is clear from figure 4 and 5 that participant 35 behave like participant 48 regarding the time of mobile applications usage whereas the difference it is very clear between participant 71 and 43 in figures 6 and 7 respectively. Also, participant 11 conduct the same behavioural profiling in most time of usage

compared with participant 74 as shown in figures 8 and 9 respectively. In addition, the overall final captured dataset statistics from the 76 participants are summarized and presented in Table 4. This amount of information was felt to be sufficiently rich to allow meaningful analysis; that is, 22,457 days of mobile usage.

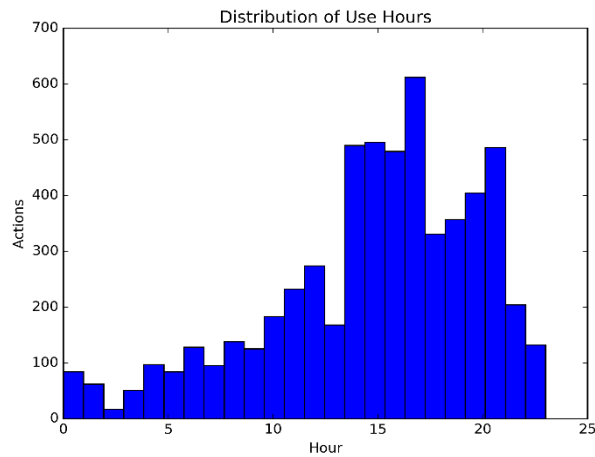


Figure.4 user 35 distribution

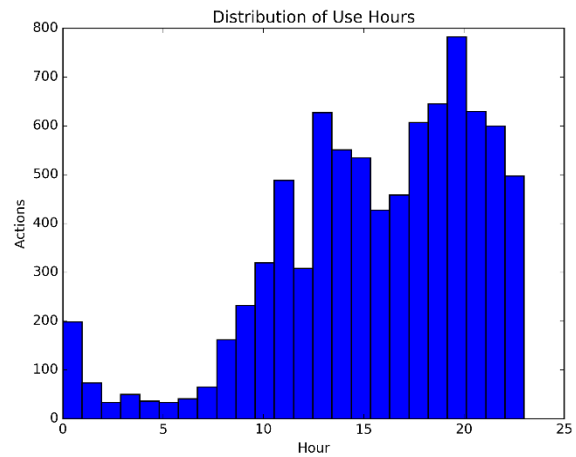


Figure 5. user 48 distribution

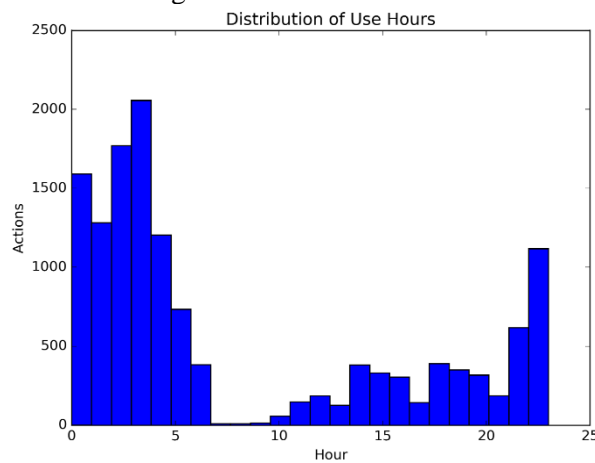


Figure.6 user 71 distribution

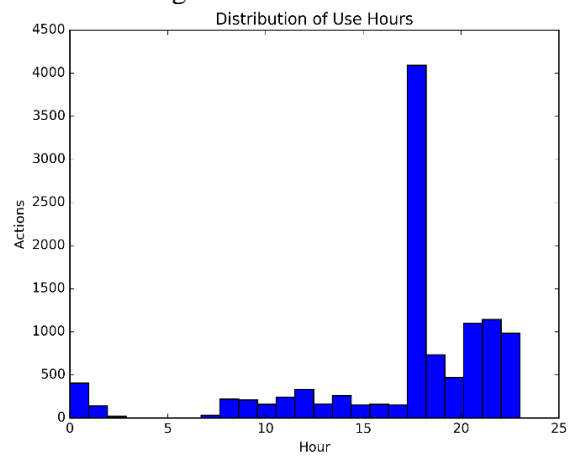


Figure.7 user 43 distribution

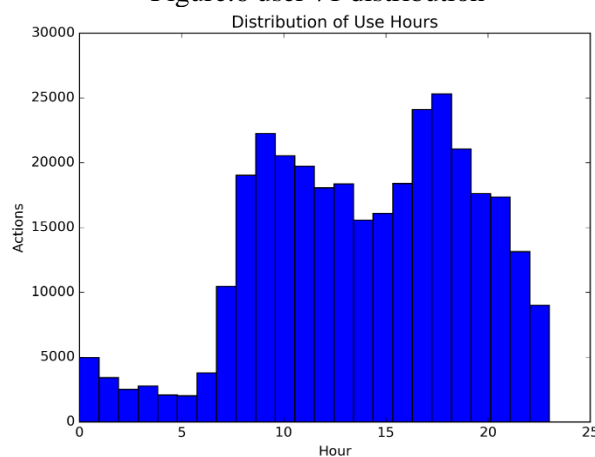


Figure.8 user 11 distribution

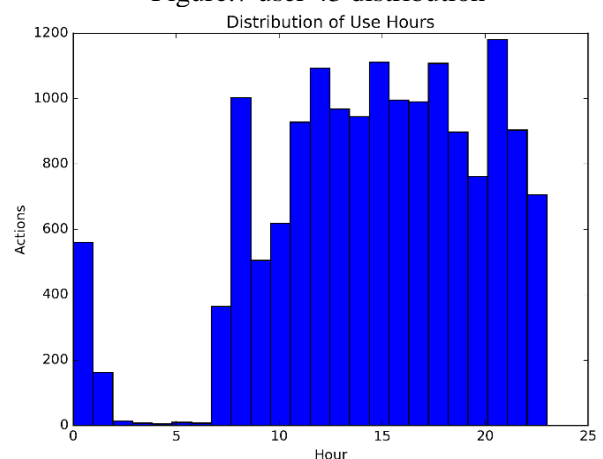


Figure.9 user 74 distribution

Table 5 shows how many sample points there were for each application. It is clear from the table that WhatsApp was the most frequently accessed application, whereas the other applications taken together were accessed a total of 252,770 times. In this context, the five most commonly used applications among the participants were WhatsApp, Google Play, SMS, Email, and Browser. Although the Viber app was ranked

second to WhatsApp in the application samples, with 118,426, as shown in Table 5, it was not commonly accessed among the participants as a whole.

Table 4: Overall final captured dataset statistics

Total Number of Users	76
Total Number of Days	22,457
Average Number of Days per User	136
Total Number of Voice Calls	101,882
Length of Voice Calls	36,566 hours
Total Number of SMS Messages	2,598,164 messages
Length of SMS Messages	124,117,633 characters
Total Number of Email Messages	14,289 email messages
Length of Email Messages	2,813,960 characters
Total Number of Actions Accessed	3,006,092

Table 5 demonstrates the total number of actions for each user for the selected applications in this dataset. It is clear from the table that the top three

ranked user actions were for WhatsApp. This in turn means that WhatsApp gained the highest amount of usage among all the participants.

Table 5: Total number of applications accessed

Application Name	Total Number of Times Accessed
WhatsApp	2,753,322
Viber	118,426
Google Photo	49,578
Camera	25,261
Email	14,289
Phone Call	13,808
Browser	10,785
SMS	8,459
Downloading	8,341
Google Play	3,251
YouTube	572

On the other hand, Table 6 demonstrates that some user action statistics regarding the 47 user actions collected. It is clear from this table that the

majority of those actions were came from WhatsApp application.

Table 6: User action statistics

Action Name	Total	Action Name	Total
Receive a text message_ WhatsApp	1,662,768	Send a text message_ WhatsApp	824,207
Receive image message_ WhatsApp	117,413	Make a free video Call_ Viber	58,784
Send free sound message_ Viber	49,578	Receive a video message_ WhatsApp	45,191
Receive image message_ Viber	43,946	Send an image message_ WhatsApp	40,939
Receive audio message_ WhatsApp	25,753	Send a location_ Viber	23,308
Take a photo_ Camera	23,308	Send an email_ Email	13,965
Receive a free call (voice/video)	12,451	Search_ Browser	10,643
Make free call(voice/video)WhatsApp	9,751	Download a file_ Downloading	8,341
Make a call_ Phone Call	7,606	Receive a sound message_ Viber	6,28
Receive a call_ Phone Call	6,202	Send a video message_ WhatsApp	6,029
Send an audio message_ WhatsApp	5,970	Receive a free voice call_ Viber	5,144
Read a SMS message_ SMS	5,101	Send an SMS message_ SMS	3,358
Download app_ Google Play	3,251	Receive a location_ Viber	2,779
Upload image_ Google Photo	1,130	Save a photo_ Camera	1,130
Receive a free video call_ Viber	1,066	Receive a PDF file_ WhatsApp	1,016
Receive a contact card_ WhatsApp	842	Delete a message_ Viber	822
Record a video_ Camera	822	Search on YouTube_ YouTube	572

Action Name	Total	Action Name	Total
Receive a location_ WhatsApp	517	Read an email_ Email	325
Update app_ Google Play	324	Send a contact card_ WhatsApp	192
Send a PDF file_ WhatsApp	162	Watch a video_ Browser	142
Make a free voice call_ Viber	139	Send a location_ WhatsApp	121
Send free image message_ Viber	10	Send a free text message_ Viber	4
Receive a text message_ Viber	1	Upload video_ Google Photo	1
Save a video_ Camera	1		

Table 7 presents an overview of all the users' data and data collection statistics, which are arranged based on the actions per hour for each user. Each user's data were stored in an individual text file and each record contains the following fields: a date in two formats: human time and a time stamp (e.g., 2016-06-28 20:22:30,

1467141750071), application name, action type, and extra information, such as message/email length and call duration. As illustrated in Table 7, a large amount of user actions took place over a small number of days, as was the case with User ID (UID) 42, which suggests that this individual might be considered a very active user.

Table 7. Data collection statistics

U	TA	TUD	APD	APH	U	TA	TUD	APD	APH
11	327,476	662	494	20	41	12,325	132	93	3
04	391,479	737	531	22	51	17,715	187	94	3
42	16,707	40	417	17	07	14,741	174	84	3
47	265,603	617	430	17	69	3,832	45	85	3
53	264,999	582	455	18	06	19,366	236	82	3
03	96,058	284	338	14	30	33,956	442	76	3
67	120,757	403	299	12	49	19,757	259	76	3
68	18,340	64	286	12	10	36,284	487	74	3
26	3,330	14	237	10	32	17,605	236	74	3
28	194,615	807	241	10	24	50,297	689	73	3
43	11,136	40	278	11	62	10,296	143	72	3
52	28,155	102	276	11	73	5,600	80	70	3
71	13,702	51	268	11	70	20,860	298	70	3
56	10,608	49	216	9	19	19,798	346	57	2
57	56,348	261	215	9	37	21,587	384	56	2
09	12,256	62	197	8	22	18,457	337	54	2
45	12,370	68	181	7	44	34,202	637	53	2
74	15,842	81	195	8	55	22,933	424	54	2
34	14,645	85	172	7	33	29,018	549	52	2
48	5,728	35	163	6	29	14,254	285	50	2
63	15,725	94	167	7	05	61,205	1230	49	2
76	28,486	165	172	7	21	21,880	443	49	2
15	16,964	107	158	6	50	21,269	431	49	2
36	46,917	323	145	6	66	47,319	984	48	2
39	24,004	160	150	6	46	27,576	592	46	1
60	22,207	149	149	6	38	14,807	333	44	1
64	10,822	70	154	6	72	15,068	346	43	1
12	8,759	62	141	5	08	14,986	343	43	1
75	5,905	46	128	5	61	14,496	361	40	1
02	14,412	114	126	5	23	6,970	175	39	1
13	39,956	319	125	5	40	10,314	261	39	1
20	21,439	168	127	5	59	4,967	138	35	1
14	24,140	211	114	4	25	4,226	131	32	1
54	30,197	262	115	4	16	20,378	644	31	1
31	20,986	195	107	4	35	8,394	271	30	1
65	7,081	69	102	4	18	8,390	280	29	1
27	8,992	91	98	4	58	10,079	349	28	1

U	TA	TUD	APD	APH	U	TA	TUD	APD	APH
01	29,463	308	95	3	17	23,523	818	28	1
U	User ID								
TA	Total Actions								
TUD	Total Usage Days								
APD	Actions per day								
APH	Actions per hour								

5. Conclusions

This study presented a new user-apps interactions dataset for behavioural profiling using smartphones in terms of mobile application security. In this research work, a study involving data collected from 76 users over a 1-month period was conducted, generating over 3 million actions based on users' interactions with their smartphone. Furthermore, 12 applications were collected with respect the user's privacy. This dataset might help researches in different aspects. For instance, studying the user behaviour interaction regarding application time usage, user authentication based on behavioural profiling biometric, prediction the next app usage to fulfil both security and usability requirements, and prediction the next action selected as well. For future work, solutions could be suggested and tested to improve the usability and security requirements of the mobile security. More specifically, data on user behaviour is gathered in the background without requiring any dedicated activity by the user, by regularly and periodically checking user behaviour in order to continuously monitor the protection of the mobile device.

6. References

- [1] Statista (2018) Number of smartphone users worldwide 2014-2020. Available at: <https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/> (Accessed: 21 November 2018).
- [2] Statista (2016a) *Forecast of smartphone user numbers in the United Kingdom) 2015-2022*. Available at: <https://www.statista.com/statistics/553464/predicted-number-of-smartphone-users-in-the-united-kingdom-uk/> (Accessed: 4 September 2018).
- [3] Statista (2016b) World wide mobile app revenues in 2015, 2016 and 2020 (in billion U.S. dollars). Available at: <https://www.statista.com/statistics/269025/worldwide-mobile-app-revenue-forecast/> (Accessed: 21 November 2018).
- [4] Comscore (2015) Mobile Metrix Reveals the UKs Top Smartphone and Tablet Destinations. Available at: <https://www.comscore.com/Insights/Data-Mine/Mobile-Metrix-Reveals-the-UKs-Top-Smartphone-and-Tablet-Destinations> (Accessed: 29 March 2015).
- [5] Clarke, N. (2011) *Transparent User Authentication: Biometrics, RFID and Behavioural Profiling*. London: Springer Science & Business Media. doi: 10.1007/978-0-85729-805-8.
- [6] Alotaibi, S., Furnell, S. and Clarke, N. (2015) 'Transparent authentication systems for mobile device security: A review', in *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. IEEE, pp. 406–413. doi: 10.1109/ICITST.2015.7412131.
- [7] Crawford, H., Renaud, K. and Storer, T. (2013) 'A framework for continuous, transparent mobile device authentication', *Computers & Security*, 39, pp. 127–136. doi: 10.1016/j.cose.2013.05.005.
- [8] Traoré, I. and Ahmed, A. A. E. (2012) 'Introduction to Continuous Authentication', in Traore, I. and Ahmed, A. A. E. (eds) *Continuous Authentication Using Biometrics*. IGI Global, pp. 1–22. doi: 10.4018/978-1-61350-129-0.ch001.
- [9] Clarke, N., Karatzouni, S. and Furnell, S. (2009) 'Flexible and Transparent User Authentication for Mobile Devices', in, pp. 1–12. doi: 10.1007/978-3-642-01244-0_1.
- [10] Zhang, J. et al. (2018) 'T2FA: Transparent Two-Factor Authentication', *IEEE Access*. IEEE, 6, pp. 32677–32686. doi: 10.1109/ACCESS.2018.2844548.
- [11] Hatin, J. et al. (2017) 'Privacy Preserving Transparent Mobile Authentication', in *Proceedings of the 3rd International Conference on Information Systems Security and Privacy*. SCITEPRESS - Science and Technology Publications, pp. 354–361. doi: 10.5220/0006186803540361.
- [12] Meng, W. et al. (2015) 'Surveying the Development of Biometric User Authentication on Mobile Phones', *IEEE Communications Surveys & Tutorials*. IEEE, 17(3), pp. 1268–1293. doi: 10.1109/COMST.2014.2386915.
- [13] Mahfouz, A., Mahmoud, T. M. and Eldin, A. S. (2017) 'A survey on behavioral biometric authentication on smartphones', *Journal of Information Security and Applications*, 37, pp. 28–37. doi: 10.1016/j.jisa.2017.10.002.

- [14] Li, F. *et al.* (2011) 'Misuse Detection for Mobile Devices Using Behaviour Profiling', *International Journal of Cyber Warfare and Terrorism*, 1(1), pp. 41–53. doi: 10.4018/ijcwt.2011010105.
- [15] Eagle, N. and Pentland, A. (2006) 'Reality mining: sensing complex social systems', *Personal and Ubiquitous Computing*, 10(4), pp. 255–268. doi: 10.1007/s00779-005-0046-3.
- [16] Li, F. *et al.* (2014) 'Active authentication for mobile devices utilising behaviour profiling', *International Journal of Information Security*, 13(3), pp. 229–244. doi: 10.1007/s10207-013-0209-6.
- [17] Saevanee, H., Clarke, N. L. and Furnell, S. M. (2012) 'Multi-modal Behavioural Biometric Authentication for Mobile Devices', in *27th IFIP International Information Security and Privacy Conference - SEC2012, Heraklion, Crete, Greece, 4-6 June, pp465-474*, 2012, pp. 465–474. doi: 10.1007/978-3-642-30436-1_38.
- [18] Saevanee, H. *et al.* (2014) 'Text-Based Active Authentication for Mobile Devices', in, pp. 99–112. doi: 10.1007/978-3-642-55415-5_9.
- [19] Fridman, L. *et al.* (2017) 'Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location', *IEEE Systems Journal*, 11(2), pp. 513–521. doi: 10.1109/JSYST.2015.2472579.
- [20] Neal, T. J. and Woodard, D. L. (2017) 'Using associative classification to authenticate mobile device users', in *2017 IEEE International Joint Conference on Biometrics (IJCB)*. IEEE, pp. 71–79. doi: 10.1109/BTAS.2017.8272684.
- [21] Shi, W. *et al.* (2011) 'SenGuard: Passive user identification on smartphones using multiple sensors', in *2011 IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, pp. 141–148. doi: 10.1109/WiMOB.2011.6085412.
- [22] Khan, H. and Hengartner, U. (2014) 'Towards application-centric implicit authentication on smartphones', in *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications - HotMobile '14*. New York, New York, USA: ACM Press, pp. 1–6. doi: 10.1145/2565585.2565590.
- [23] Hayashi, E. *et al.* (2012) 'Goldilocks and the Two Mobile Devices: Going Beyond All-Or-Nothing Access to a Device's Applications', in *Proceedings of the Eighth Symposium on Usable Privacy and Security*. New York, New York, USA: ACM Press. doi: 10.1145/2335356.2335359.
- [24] Gupta, S., Buriro, A. and Crispo, B. (2018) 'Demystifying Authentication Concepts in Smartphones: Ways and Types to Secure Access', *Mobile Information Systems*, 2018, pp. 1–16. doi: 10.1155/2018/2649598.
- [25] Kayacik, H. G. *et al.* (2014) 'Data Driven Authentication: On the Effectiveness of User Behaviour Modelling with Mobile Device Sensors', in *Proceedings of the Mobile Security Technologies Workshop*. Available at: <http://arxiv.org/abs/1410.7743> (Accessed: 9 April 2019).
- [26] Acien, A., Morales, A., Vera-Rodriguez, R. and Fierrez, J. (2019) 'MultiLock: Mobile Active Authentication based on Multiple Biometric and Behavioral Patterns'. Available at: <http://arxiv.org/abs/1901.10312>.
- [27] Android (2019) *Android Debug Bridge (adb)*. Available at: <https://developer.android.com/studio/command-line/adb> (Accessed: 2 January 2019)
- [28] Tan, C., Liu, Q., Chen, E. and Xiong, H., (2012). Prediction for mobile application usage patterns. In Nokia MDC workshop (Vol. 12).
- [29] Huang, K., Zhang, C., Ma, X., & Chen, G. (2012, September). Predicting mobile application usage using contextual information. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 1059-1065). ACM.
- [30] Yan, T., Chu, D., Ganesan, D., Kansal, A., & Liu, J. (2012, June). Fast app launching for mobile devices using predictive user context. In Proceedings of the 10th international conference on Mobile systems, applications, and services (pp. 113-126). ACM.
- [31] Zou, X., Zhang, W., Li, S., & Pan, G. (2013, September). Prophet: What app you wish to use next. In Proceedings of the 2013 ACM conference on Pervasive and ubiquitous computing adjunct publication (pp. 167-170). ACM.
- [32] Liao, Z. X., Lei, P. R., Shen, T. J., Li, S. C., & Peng, W. C. (2012, December). Mining temporal profiles of mobile applications for usage prediction. In 2012 IEEE 12th International Conference on Data Mining Workshops (pp. 890-893). IEEE.
- [33] Pan, W., Aharony, N., & Pentland, A. (2011, August). Composite social network for predicting mobile apps installation. In Twenty-Fifth AAAI Conference on Artificial Intelligence.
- [34] Krishnaswamy, S., Gama, J., & Gaber, M. M. (2012, July). Mobile data stream mining: from algorithms to applications. In 2012 IEEE 13th International Conference on Mobile Data Management (pp. 360-363). IEEE.