User's Data Security Awareness in Smartphone within the Context of Pakistan

Zeshan Qureshi†, Khaid M. Awan †† and Peer Azmat Shah

Department of Computer science, COMSATS institute of information technology Attock 43600,Pakistan

Abstract
Mobile phones are the main source of communication. Fundamental purpose of the mobile phone is to communicate verbal messages from one place to other. In the present era, as we know that microelectronics has changed the world into an electronic sphere and rest of the paradigm has been filled with the modern communication techniques. With the emergence of internet, the functionality of the cell phone has changed, now cell phone are same as hand-held computers which support full functionality of a modern computing requirements as well as communication needs. The cellular phones are not only the cell phones but now have become Smart phones. One of the main challenges of the modern era especially in developing countries like Pakistan is the awareness about the security issues of the private information about the user of smart phones. Hundreds of applications have been developed for different purposes which may directly or indirectly effect the personal information of the Smartphone holder. The purpose of my research is to evaluate and identify these issues in the context of Pakistani population. There is a clear distinction among the categories of different communities of the Pakistani population along with their different needs and scenarios of using Smartphone.

Keywords:
End User Data security, Smartphone, Authentication, Personal Data

1. Introduction

According to international research, the users of the Smartphone including students, working professional from different ethnic groups, language and areas believe that the Smartphone has become a main source of information as well as a reliable medium of storing their information and data. According to general perception, the data stored in Smartphone is safe and under their personal custody [1]. Due to the same multidimensional capability of Smartphone the import of the devices has largely been increased in past few years. Smartphone applications are provided to the users through centralized data sources or repositories and are available through different app stores, normally not in a case of PC software [2]. These repositories may be official (provided and maintained by the Smartphone companies and their OS platform) or may not (Amazon App store).

Different applications follow different security models depending upon the Smartphone platform containing permitted source licensing agreement and target locations. In addition with this many applications provide application note (vetting) while installing them. At the same time the frequency of downloading a specific application form an app store plays in important role as well. The increasing number of downloads always attract hackers to mess with that particular application. Only the technology cannot guarantee the secure data manipulation in Smartphone alone. The user behaviour along with technical features play important role in maintains the secure environment in data security paradigm. Human aspects are very important along with these Platform-provided features [3]. For the better understanding of these issues, increasing the awareness and knowledge of the users can play an important role in attaining the desired goal [4].

The purpose of this research is to create awareness and highlight the main security issues and features within the context of Pakistan. The community of the country belongs to different areas and social backgrounds. This research also reveals the current behavior along with some misconceptions and overconfident trust on different repositories as well as with different applications.

2. Literature review

Personal information about a person is a valuable asset. Possession of the data plays an important role for the Soule of security. The information security is actually means that the person about which data is maintained is the only authorized entity that can alter or change the data. However some departments are free to maintain data about another person and they are no legally answerable to the law. These departments may include National security agencies, medical research centers and law enforcement departments. However other then these departments, the data of a person has to be secured by others organization as well as by the person itself. Unauthorized deletion, modification, alteration, disclosure, use and access of the data are illegal.

According to Pakistan Advertiser's Society (PAS)[5], 35% of the Smartphone users are using low cost Smartphone. Due to launch of 3G and 4G in

Manuscript received June 5, 2026
Manuscript revised June 20, 2026
https://doi.org/10.22937/IJCSNS.2026.26.6.10

Pakistan, Smartphone users have increased rapidly; cell phone user's age is normally ranging from 14 to 45 and they prefer to own Smartphone. On the other hand due to the launch of android based Tablet PC, lower age users have also been increased. Children prefer to play games on tablet PCs rather than Desktop PCs. Home PCs are becoming less functional as compared to smart phones. Most of the applications developed today are well suited in Smartphone and provide full fledge functionality related to Word processing, database management, contact management, book keeping cloud computing and distributed data management. But important question arises here that Are the Smartphone more secure and safe for these operations as compared to the Home PCs? According to [6], research conducted in 2102, 19% of peoples consider the data more private, 59% consider as private as Home PC, 19% consider less private and 2% don't know the answer.

According to a report published [3], Pakistan will have 40 million Smartphone by the end of 2016. According to [5], 35% Pakistani use cheap or low cost Smartphone due to safety and street crime issues. 60% Pakistani prefer to use more than one phone. 78 % of the people store text messages in their cell phone, 82 % people maintain their contact information in their cell phone, and 75 % people keep their photos and videos in their cell phones [3]. The results create an alarming situation because all the information stated above is consider ultra private.

People are very less willing to perform activities that deal with economic matters like managing bank accounts, e-commerce or M-commerce involving credit card transactions, using their Smartphone [7]. People are more concerned to implement security features on their Smartphone that are not even considered on their personal computer or laptop. This behavior shows an opposite trend. People do so because they prefer to use cell phone for more activities rather than laptops or PCs because cell phones provide more mobility and easiness of connectivity.

2.1. **Features related to Security**

Numbers of additional feature have been added to the Smartphone, and the process is still going on. These features may affect the security of the data stored in it as well as the Smartphone as hardware itself. Mobility, types of sensors like accelerometer, gyroscope, proximity and connectivity options like Wi-Fi, Bluetooth are the main advancements that are related to the security threats [4]. GPS in a cell is an effective and useful facility but it may also affect the personal security and privacy.

2.2. **Authentication Methods**

Different authentication methods are embedded in Smartphone to prevent unauthorized access to the device. PIN (Personal identification Number) is commonly used in relatively old dated Smart phones. Authenticity of the PIN is a question itself however it depends upon the selection of the users but still considered as an easy method for batter security. Pattern lock is a new authentication and safety features embedded in smart phone of the modern age. This pattern may have weaknesses also, depending upon the selection. Security code is another security feature somehow similar to PIN. Fingerprint reading is a latest and modern feature embedded into the devices for authentication.

2.3. **System Risk Strategies for security Implementations**

There are four different steps included in strategy of System protection defined by Security Action Cycle: Deterrence, Prevention, detection and recovery [8]. Deterrence includes the rules, policies and guidelines for the security of the data. These are fully dependent upon the user's will. Next step is Prevention which includes terms and conditions, guidelines, steps of actions and to-do list that is generated to prevent any hazard related to data security breach and theft. Detection includes the steps of action if the breach is detected. If an attack or hacking is detected, the strategies are defined to gather the information about the type of breach, identifying the target of the breach, list of theft and correlated issues that may occurs due to the breach.

Prevention and detections is technology dependant. These two sections are normally performed by the technical development features in the gadget [9]. A farmer cyber Security chief of white House has a clear objective related to the Smartphone security issue. According to his point of view, Smart phones and application related to it are a serious threat to the security [10].

2.4. **Theories for Behavioral Information Security**

Human behaviour plays an important role in adopting the security features. This adoptability is dynamic in nature as education and social value may change them accordingly. End user's general knowledge is a prime factor in information security [11]. According to TRA (Theory of respond Action or The Theory of Extended planned Behaviour, the stronger intentions create stronger actions. Action of a person are totally self controlled and self managed [12],[13]. GDT (General deterrence theory) implies that the action or behaviour of a person is a result from another fearful threat [14]. The

theory is related to the actions performed by some of the Smartphone users related to malware and spam attacks. In the field of computer science this types of threats are called Virus Hoax. TAM (Technology Acceptance Model) specifies the modular behaviour that how users can adopt themselves according to the technology [15].

2.5. **Threats, Worries related to Smartphone**

Primary concern about the Smartphone is different for different users depending upon gender, age group, professional, society and educational level. Main issues related to this factor are:

Physical loss of cell phone, theft, physical damage to the hardware, loss of data, battery life and careless connectivity to some network without proper authentication [7]. Physical loss of the Smartphone may result in total loss of the data if not shared by other devices. Physical damage is not considered as a breach of the security. Battery life of the cell phone may restrict user to avoid heavy and large applications to run due to the fear of roll back transaction in case of full power loss. People using smart phone avoid using online transactions which involves a plenty of authentication and verification due to limited battery life. People also avoid filling detailed farms and surveys using their cell phone for the same reason.

Unauthenticated connectivity to some network is a hot issue for the security of the device connected. Some network voluntarily invites the users to connect with them, as they can get a gateway for the breach in the connected devices.

2.6. **Smart phone security Features**

Security and authentication validation methods are almost same like in PCs. Some of the vendors of Smartphone have introduced new security features which include Pattern draws. The user first save a specific pattern by joining points in a matrix, then each time for the login, same pattern has to be drawn. Pattern has a lot of security hazards which are discussed in this paper.
Another option is fingerprint detection. The device allows the user after verifying the finger print of the user.

2.7. **Application repositories and stores**

Popularity of Smartphone is directly dependent upon the facility of using multiple applications. Now days, billions of application have been developed for the Smartphone which are dependent upon users. Authentication of application is directly connected with the type of OS for which that application is developed. Android is an open source OS for the Smartphone. Billions of applications have been developed for android based Smartphone. There is a problem that android is an open source OS. The ratio of spam and malware attack has increased for the android. Second reason for the increased attack is that the OS is considered most popular one especially in Pakistan. The installation of third-party application has different perspective for different smart phone vendors. It depends upon the amount of control a vendor wishes to allow for the user [16]. There are two main approaches being used for the application repositories.

- A *closed platform* also known as *close ecosystem* or *walled garden* approach. According to this approach the main privacy and authentication is controlled by the vendor. A user can only install an application; he has no control over the privacy or authentication of the application.
- The other one is *End user control model*. In this model, authentication and security for an application is the sole responsibility of the user. A user can install, change or modify the application according to his/her custom needs.

3. Research methodology

Purpose of this paper is to explain and create awareness regarding personal data security related to Smartphone. Survey strategy is used in this paper for the elaboration of the problems, threats, issues and ground realities present in the developing country like Pakistan. The conclusions and results are obtained by the explanatory answers against the research questions within the context of Pakistan.

3.1. **Research questions**

- Do people realize the nature of security threats or risks?
- Do people know the trustworthy application repositories for downloading applications?
- Does the education level matters for the secure use of the gadget?
- Do people know different features of security options given in their Smartphone?

3.2. **Instrument used for research and data collection**

Printed questioners were distributed among the target audience containing the related questions. Online face book based research questioner for the survey was also launched through an application hosted by the

facebook [17]. The survey contains the important questions related to the smart phone trend and security options adopted by the users. This survey was very helpful in getting the feedback from the audience specially age ranging from 15 to 35 showing behaviour of the youth towards Smartphone. Interview method was also adopted for the collection of the data targeting the audience especially from age 30 and above which gives the throughput from that age group. Telephonic calls were also made to get the data from the users.

3.3. Target Population: Sampling

Sampling include almost every type of person including businessman, teacher, lawyer, doctor, labourer, shopkeeper, hose hold ladies, students of SSC,HSSC, and graduate level. The age range of the people was from 14 to 55. Total 1287 responses were recorded form the samples. Although the sample is short but the trends directions are clear. Total 645 responses are recorded through phone calls, 140 responses through printed questioner, 40 are recorded through facebook questionnaire and 462 responses were recorded by interviewing the people.

4. Data analysis

From the initial 1287 responses, people were included from various educational levels. 27 % of the people are of Master degree holders. 41 % people were literate up to Graduate level, 17% were of grade 12 or intermediate level, and 14% people were qualified up to matriculation level as shown in the Fig. 1(a).

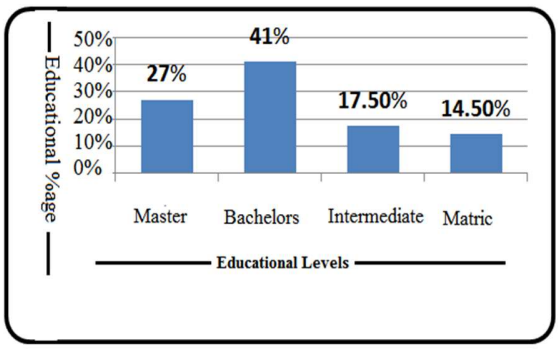

Figure. 1(a) Educational level of Smartphone Users

On the other hand Fig 1(b) shows the derived age range of Smartphone users form the samples. People of age ranging from 5 to 30 prefer the use of Smartphone due to features provided hence covering larger percentage of 41 %. Relatively older aged people do not prefer Smartphone as they find its handling and usage bit difficult. Their primary concern is to call and message only. Very few people are found using Smartphone in the age range above 60 years. These are the people who have a technical background and better educational level.

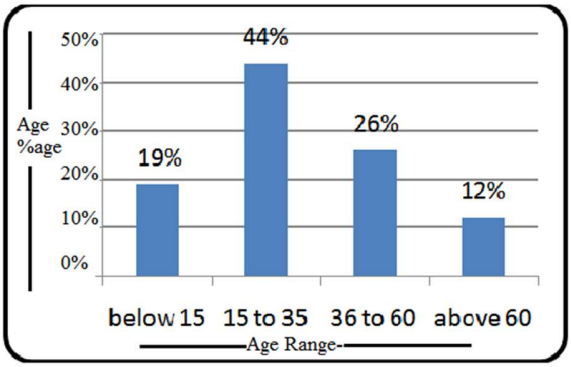

Figure. 1(b) Age Range of Smartphone users.

4.1. **International Data and Facts**

According to the statistics presented by[18] in Table A given below, the division of internet users with respect to internet connectivity is described.

Table 1. Types of internet connections usage [18]

Internet Connection type	Percentage
Mobile Data	82%
Home Wi-Fi	64%
Public Wi-Fi	35%
Broadband	16%
Cable	03%
Others	02%

82% of the users of the smart phone use Mobile Data for internet connectivity. Home Wi-Fi users are about 64%. 35% users use internet through Wi-Fi on public places. 16% users use internet through Broad Band connectivity, only 03% users use internet through cable services and 02% use other methods to connect with the word through internet.

4.2. **Current Data Analysis**

According to the data collected for the specified purpose, 56 % users for the Smartphone are male and 44% are female as shown in Fig. 2.

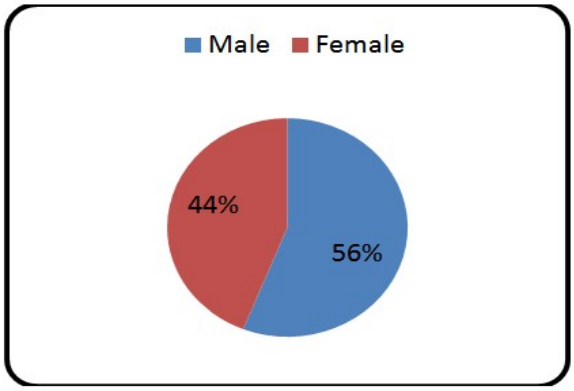

Figure. 2. Gender based division of Smartphone Users;

72.7 % of the Smartphone users use the Android based cell phones. 22.3 % users are using IOS based Smartphone and 4.70 % are using windows Smartphone as shown in Fig. 3.

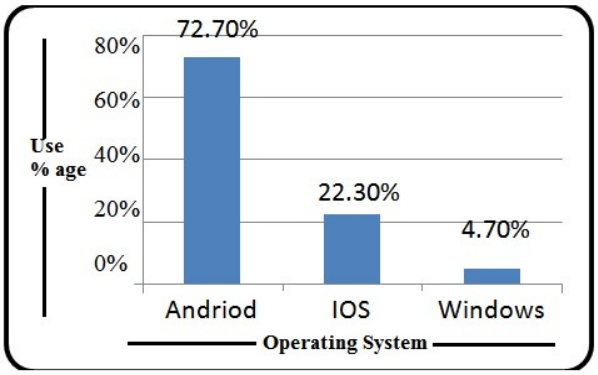

Figure. 3. OS based Smartphone Users.

One of the important observations recorded is about the security feature of the Smartphone. As shown in Fig. 4, 11 % people use PIN (Personal Identification Number) as a security lock. 59% use Pattern Lock for the safety for their Smartphone data and access. 19 % people use Password and 08 % use Fingerprint identification and authentication method. On the other hand there are 4% people who are not using any locking system for their Smartphone.

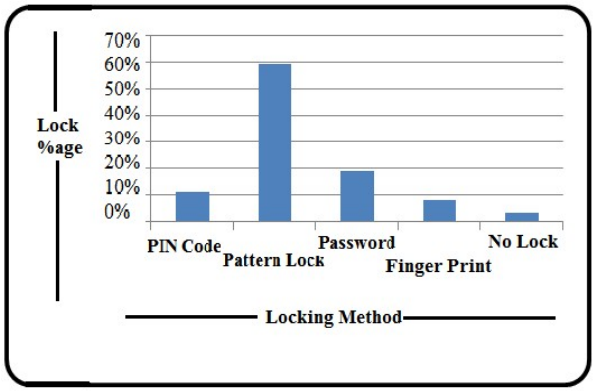

Figure. 4 Screen Locking Methods

Due to an open source operating system, hundreds of thousands applications have been developed for Android based OS. As majority of the people are using this OS embedded in their smart phones, less attentions is paid toward the In-App security permissions while installing an application. Fig. 5 clearly show the picture related to the scenario.

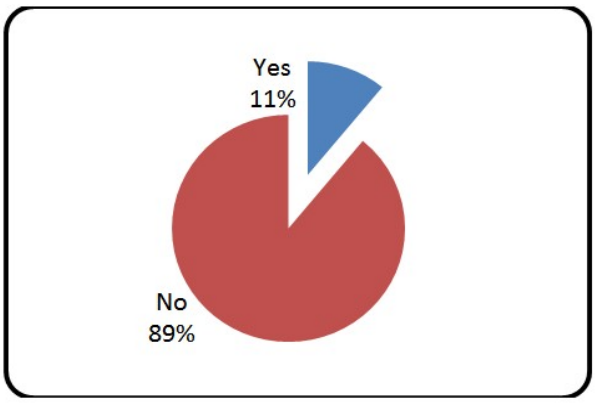

Figure. 5. In-App Security and Licensee Agreement Response.

Only 11 % people said that they, somehow, pay attention to the License agreement and installation notes while downloading and installing applications from play store. On the other hand 89% people do not pay any attention to this feature at all.

4.3. **Security breaches classifications**

Security related to the smart phone is divided into two main categories. First is intentional Ignorance in which users intentionally ignore security risks. In this case risks are well-defined and clear but people bypass these features. This may include improper or weak PIN selection, commonly known passwords usually containing first or last name and common numerical

values like phone numbers. It also includes ignoring security features of some applications. Second category is Unintentional ignorance. Sometimes people are unaware of some security threats. Accepting license agreements without reading it and installing an application from unknown or unreliable source can create serious security issues. According to the categories described above, security threats are divided in three types:

- Operating System Embedded Security Breaches **(OSESB)**
- Online Application Security Breaches **(ONLASB)**
- Offline Application Security Breaches **(OFFLASB)**

OSESB are the type of security breach includes the weaknesses of Operating Systems due to which security breach is possible. It includes the security options provided by the OS. ONLASB are the security risks while using some online application. During the installation or using them online, servers may access your personal information secretly. The user is totally unaware of these features of the applications.

OFFLASB may include security risk that may arise by using some applications even running offline. These types of application can collect user secrete information silently and storing them into some kind of buffer. As soon as the user's devices get connected to the internet, it may start transferring this information to some server.

5. Recommended solutions for security breaches

According to the security breaches mentioned in section 4.3, following outcomes and recommendations against each type is given comprehensively.

5.1. **OSESB handling**

As shown in the results in Fig .3, majority of the people are using Android because of its user-friendly interface and free applications availability. Bugs, spam and malware are frequent in Android regardless of the version we use. Many flaws have been highlighted in the android systems as described in [19], these types of flaws come under the type of OSESB. As compared to Android, Apple IOS and Microsoft Widows OS are considered safer. But due to the limited stack of applications they are not widely used in Pakistan.

5.2. **ONLASB handling**

Many applications have been developed that use (VoIP). However no one can deny the benefits of these but on the same time some applications have been reported as a serious threat for their users. These applications can secretly gather personal information about the user and transmit them to the server.

Viber is officially banned for the government officials. Pakistani government has decided not to use Viber for official and unofficial communication[20]. It is developed by an Israeli company Viber Media. Most of the VoIP application developer companies have the ability to monitor and keep records of the user's data for those who are using their application. These types of security risks are covered by ONLASB. Android is facing a great threat of malware applications. *Malware* also come under ONLASB, as described in[21], these type of applications are developed to disturb the user, breach into user data for either manipulation of the data or to steal the information and to damage the device. Other types of applications may include *spywares* and *Gray-wares* which are also designed to collect personal information and data of the users.

5.3. **OFFLASB handling**

Some of the applications may not require internet connection for their executions. Normally those applications which require filling some data form while a user is working offline may put that information in a buffer waiting for transfer as soon as they got internet connectivity. But luckily these types of applications are not as risky as compared to ONLASB.

5.4. **Some additional recommendations**

Based upon the security issues and breaches discussed in the previous section, some recommendation are given below for eliminating or somehow minimizing the effect of data lost for a smart phone user.

5.4.1. Irregular and excessive permissions

Simple application requires simple and less permission but if an application is requesting to access some core information frequently then that application is malicious. For example while downloading a simple wallpaper application, if it requires the access the secure area of the OS or device functionality features then the application is risky as it do not make any sense to access those functional areas of the device for wallpaper application. So try to avoid such applications which require these types of permissions.

5.4.2. Similar named applications

Sometime hackers develop the malware or spyware which resembles with the icons and name with some existing and well known application. By the first look a user cannot identify the application as a real or fake one. Always verify the repository first, then the developer profile before downloading an application.

5.4.3. Improper authentication for applications

While downloading some applications, it may require some authentication to carry out the process. Now most of the application's authentication criteria are collaborated with the facebook and email ID for the sake of saving time and reducing complexity for the user for filling entire form again and again. On the other hand this facility has gained the hackers' interest also. Some un-trusted applications may ask to access the existing account information as well. Always be vigilant in using applications which require same credential for the log in.

5.4.4. Pattern locks smudge effect

According to the data collected, most of the people use patter locking as authentication criteria for their Smartphone. That is because of the new features added in cell phone when they are transformed into a smart phone and touch screen sensitive input methods. However this method of authentication is more risky as it can be judged relatively easy as compared to pin code and password.

Figure. 6 Showing Smudge effect of Pattern Lock

As shown in the Fig. 6, pattern lock may leave a smudge effect on the screen which can be viewable through some angle. It is recommended to use a complex pattern that may involve same points of pattern to be touched more than once as shown in Fig. 7.Also keep on changing pattern time to time.

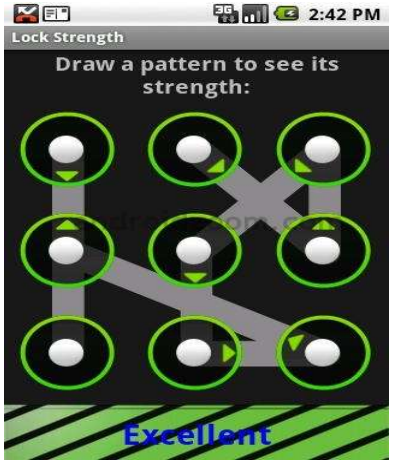

Figure. 7 Pattern strength

Besides the recommendations stated above, following suggestions are also given for the security of personal data of user in smart phone.

- Do not use un-trusted repositories for downloading application.
- Always check the developer's profile and rating before downloading some application.
- Go through the comments given against the application to judge its status before downloading.
- Do not allow anonymous requests for connections on your Smartphone.
- Try to avoid unknown Wi-Fi routers even if they are free to connect.
- Do not accept any security configuration setting from unknown source.
- Always use updated versions for the all the applications.

6. Conclusion

Users of Smartphone in Pakistan are increasing in numbers exponentially. As the advancement in microelectronics is tremendous in its nature, vendors of the devices are competing with each other at the same time. The research shows that in the race of technology, some security features are neglected by the manufacturer. But the main responsibility lies with the user. Even most of the Smartphone users are educated, but they intentionally bypass the security measures provided by the device. There is a dynamic relation between educational level and age range of Smartphone users.

There is a less count in percentage of the people above 60 years of age, who do not possess good educational status. Most of old aged people are reluctant in using feature Phones. They prefer simple ones due to ease in operating. The research finds that the user behaviour and importance of the security awareness is mandatory for the protection of personal data. Gender does not play any significant role in maintaining security. It is revealed also that OS dependency is crucial in Smartphone. Types of access method for different OS in smart phones may also affect the security issues. Updated and trusted applications can be proved as trustworthy.

References

[1] B. H. Jones and L. R. Heinrichs, "DO BUSINESS STUDENTS PRACTICE SMARTPHONE SECURITY?," *J. Comput. Inf. Syst. Winter*, 2012.

[2] A. Mylonas, A. Kastania, and D. Gritzalis, "Delegate the smartphone user? Security awareness in smartphone platforms," *Comput. Secur.*, vol. 34, pp. 47–66, 2013.

[3] F. Baloch, "Studying Pakistan's growing obsession with smartphones - The Express Tribune." Express Tribune, 2016.

[4] S. Vongsingthong and S. Boonkrong, "A survey on smartphone authentication," *Walailak J. Sci. Technol.*, vol. 12, no. 1, pp. 1–19, 2015.

[5] "Smart Phone Usage in Pakistan [Infographics] | Pakistan Advertisers Society." .

[6] J. M. Urban, C. J. Hoofnagle, and S. Li, "Mobile Phones and Privacy," *UC Berkeley Public Law Res. Pap. No. 2103405*, p. 33, 2012.

[7] E. Chin, A. P. Felt, V. Sekar, and D. Wagner, "Measuring user confidence in smartphone security and privacy," *Proc. Eighth Symp. Usable Priv. Secur. - SOUPS '12*, no. 1, p. 1, 2012.

[8] D. W. Straub and R. J. Welke, "Coping with systems Risk: Security Planning Models for Management Decision Making," *MIS Quaterly*, vol. December, no. 4, pp. 441–469, 1998.

[9] "Impact-of-Negative-Message-Framing-on-Security-Adoption.pdf." .

[10] Former Cyber security Czar Clarke, "Cyber Security Chief," *Network World*, 2011. [Online]. Available: http://www.networkworld.com/%0Anews/2011/091911-clarke-cybersecurity-251014.html.%0A. [Accessed: 19-Sep-2011].

[11] C. Colwill, "Human factors in information security: The insider threat - Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, 2009.

[12] M. F. Icek Ajzen, "An introduction to theory and research," vol. 10.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.

[14] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann, and B. Hohler, "Employees' information security awareness and behavior: A literature review," *Proc. Annu. Hawaii Int. Conf. Syst. Sci.*, pp. 2978–2987, 2013.

[15] M. Chuttur, "Overview of the Technology Acceptance Model: Origins , Developments and Future Directions," *Sprouts Work. Pap. Inf. Syst.*, vol. 9, no. 2009, pp. 1–23, 2009.

[16] D. De Atley and S. Cooper, "Secure software installation," p. 20, 2012.

[17] Z. Qureshi, "Facebook Survey." [Online]. Available: https://apps.facebook.com/my-surveys/form/personal-data-security-on-smartphon?from=admin_wall.

[18] N. Nazri, N. Azian, and J. Ibrahim, "Survey on Mobile and Wireless Security Awareness : User Perspectives," vol. 4, no. 1, pp. 1287–1292, 2015.

[19] J. E. Dunn, "Android's 6 biggest security flaws 2016." [Online]. Available: http://www.techworld.com/security/androids-6-biggest-security-flaws-2016-3622116/. [Accessed: 04-Dec-2016].

[20] A. Atta, "Pakistan Bans Viber for Government Officials," 2014. [Online]. Available: https://propakistani.pk/2015/03/19/pakistan-bans-viber-for-government-officials/. [Accessed: 15-Dec-2016].

[21] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," *Proc. 1st ACM Work. Secur. Priv. smartphones Mob. devices - SPSM '11*, pp. 3–14, 2011.