International Journal of Automation and Computing 13(4), August 2016, 350-363
DOI: 10.1007/s11633-016-1011-5

Conceivable Security Risks and Authentication Techniques for Smart Devices: A Comparative Evaluation of Security Practices

Syeda Mariam Muzammal[1] Munam Ali Shah[1] Si-Jing Zhang[2] Hong-Ji Yang[3]

[1]Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan
[2]Department of Computer Science and Technology, University of Bedfordshire, Luton LU13JU, UK
[3]Centre for Creative Computing, Bath Spa University, Bath BA2 9BN, UK

Abstract: With the rapidly escalating use of smart devices and fraudulent transaction of users′ data from their devices, efficient and reliable techniques for authentication of the smart devices have become an obligatory issue. This paper reviews the security risks for mobile devices and studies several authentication techniques available for smart devices. The results from field studies enable a comparative evaluation of user-preferred authentication mechanisms and their opinions about reliability, biometric authentication and visual authentication techniques.

Keywords: Smart devices, security risks, authentication, biometric, privacy.

1 Introduction

Smart devices are ubiquitous in the present world. The new-generation smart devices, e.g., Apple′s iPhone series and Google Android based systems, have become successful in accomplishing many of the users′ tasks that required a personal computer previously. People use smart devices not only for the general purpose of cell phones but also for staying connected to the Internet and social media as well as for enjoying the latest mobile applications, several entertaining games and flourishing, online and offline, multimedia services[1]. With the enhanced and advanced functionalities, smart devices carry a large amount of user′s private and confidential data with the risks of being lost and theft. For this most common device of communication around the world, the need of a reliable authentication mechanism is of utmost importance in order to protect the data and privacy. Though there are many other potential threats for smart devices, such as data leakage via network (e.g., through a social website) and unauthorised malware attacks[2, 3] by smart phone open source applications since smart devices almost always stay connected to a public network and a significant amount of user′s data is accessible to these applications and potentially others[4], in this paper, we will focus only on the authentication of a smart device. An advanced and reliable authentication mechanism might save user privacy from increasing issues of robbery and theft of device[5] and misuse of users′ sensitive data. This will also increase users′ confidence level to make full use of all the features of a personal smart device.

Although numerous authentication techniques are provided by the smart devices for protection from unauthorised users, smart device users still require an advanced level of privacy protection for information stored on their mobile devices[6].

There are many types of security methods used in smart devices and most common methods include personal identification number (PIN), passwords, patterns, fingerprint, face recognition and various other biometric authentication techniques being embedded in mobile devices. Passwords have served us well for many years, but they suffer from a number of problems that suggest their sovereignty should be coming to an end[5, 7]. The visual authentication techniques especially passwords and PIN are not considered as secure and reliable among the smart phone users[8]. Users frequently forget passwords and PIN, due to which they try to keep copies of their passwords[2] in other media, increasing the possibility of unauthorised attacks on their privacy. Also, users tend to keep using the same password for other devices or in other places, and due to the static nature of passwords they invite repeated attacks of illegal access to their private data on the device. Another technique most widely used in smart devices is the use of pattern recognition (Fig. 1 (a)). The user sets a pattern to authenticate the device and still needs to remember the specific pattern. This indicates that the visual authentication techniques in smart devices do not guarantee a person′s identity in case of being stolen or hacking of passwords or patterns. Some devices ask for the email ID and password after some unsuccessful attempts of authentication (Fig. 1 (b)). Another limitation of visual passwords and patterns is that since

Research Article
Manuscript received July 22, 2014; accepted December 2, 2015; published online June 29, 2016
Recommended by Associate Editor Jangmyung Lee

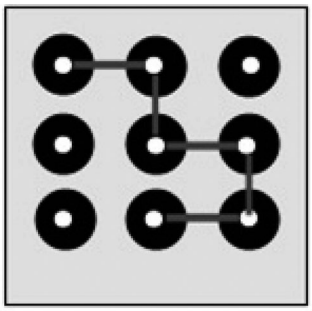
they are based on the knowledge of the user, so an unauthorised access is possible by guess, sharing with people or writing them somewhere for remembrance. This happens to security cards or tokens such as passports, ID cards or credit cards. What if the card is misplaced somewhere or stolen by someone? Then one will not be able to access his/her device. This indicates that these knowledge-based approaches are not much satisfactory for authentication security.

Other than the traditional security practices, biometric security[9] identifies an individual based on physical characteristics, i.e., what the user is rather than what the user possesses or remembers[10]. Biometric security techniques in smart devices include physical human identifiers like fingerprint scanning and face recognition, whereas retinal scanning is supposed to be shortly available in smart devices. These human traits can be accurately captured using sensors and devices, and they are distinctive to each individual, and can neither be copied nor stolen. Despite of these techniques, voice recognition and signature analysis are also of great interest for security concerns. Some advantages and disadvantages of biometric authentication techniques applied so far in smart devices are shown in Table 1.

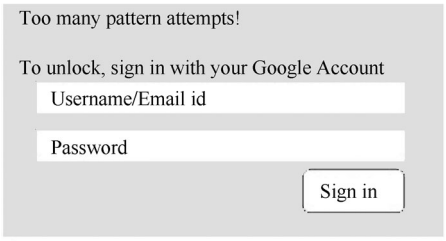
Smart devices may contain sensitive and confidential user data, leading to greater chances of theft and loss of mobile devices. For this reason, the need for a smart and advanced authentication technique has become a necessity of the smart device users. Any authentication technique applied must be able to protect users′ privacy and ensure the prevention of unauthorised access to the smart device.

An adaptive solution to secure the authentication process of cellular phones using gait and location tracks of owner has also been proposed[11]. Apple has recently introduced fingerprint authentication in smart phone device iPhone 5s with the claim that "it is a convenient and secure way to access your phone". Table 1 shows a comparison of different security and authentication techniques applied commonly in smart devices so far.

There are some pros and cons of everything; and same is the case with technologies of authentication and security. The main difference between the biometric security and visual based authentications is that biometrics is based on what the user is whereas visual techniques depend on what the user remembers.



(a)



(b)

Fig. 1 Pattern and password recognition authentication in smart devices

In this survey we are going to analyse the preferred authentication mechanisms for smart device users among all the authentication techniques implemented so far by the smart device manufacturers. This study will also be helpful in measuring users′ confidence levels for using an authentication technique, how much users rely on a specific authentication technique, and what they prefer for the security of private and confidential data on their smart device.

2 Related work

The propagation of smart phones as a multipurpose device has made it prone to more risks and security threats. The risks to confidential data in personal smart devices can be divided into two broad categories: unauthorised access

Table 1 Authentication methods in smart devices

Factor	Examples	Advantages	Disadvantages
Information based	-PIN/Password -Pattern recognition -Security question -Email-ID and its password	-Low cost -Easy to manage -No extra hardware required	-Security depends on strength of Password/PIN. -Can be easily guessed, stolen, forgotten, or disclosed.
Biometrics[9]	-Fingerprint -Voice recognition -Face recognition -Ear recognition -Iris/Retina scanning	-Easy to use -Need not be remembered -Cannot be passed on	-Biometric factors are subject to change, e.g., voice changes with age, etc. -Might violate data protection legislation[16]. -Some biometric authentications, like fingerprint/eye verification, require specified and advanced hardware or sensors to be embedded in the smart device.

to data and data loss[12]. Due to the increased and advanced functionalities and features, users have their personal and other confidential stuff stored in the smart devices which make them more attractive to attackers. Hence, traditional risks, like theft and fraud, are likely to occur with increased impact, and the same with the advanced threats like using the location capabilities of a smart phone for inspection or supervision of an individual[13].

Smart phones can be considered as smart adaptation of computers with ever-present and smartly developed features of a mobile phone[14]. Smart phone users also store a vast array of different data on their devices, from personal call logs to messages (maybe in the form of emails, short message service (SMS), multimedia messaging service (MMS)), contact lists, addresses, birth dates, audios, videos, photos, notes and various other files based on the usage of the smart phone[14]. From the business perspective, businessmen use smart phones for communication with the clients, for business deals, to send some sensitive information to the partners and for a number of useful and important tasks. Such users would always feel insecure when they are away from their devices.

In recent past, smart phones were being mostly used for business purposes, but in current era, all age groups, particularly above 16, are using smart devices for specific purposes. As the use of smart phones has increased overall, the level of security threat has also arose. It is mandatory to secure one′s device with one or more authentication(s). Negligence on part of the user can lead to security holes enabling hackers to track the user′s activities, and the visited links, leading to an increased threat of successful attacks.

User authentication is considered the most effective practical method as a safeguard for vulnerable data in smart phones, so that the efficiency and usability of authentication schemes for the smart devices are among hot topics in the field of research and development (R&D)[14, 15].

Most of the users are disinclined towards the intricate authentication schemes like a strong passcode, whereas the simpler schemes are not very effective from the security point of view[15]. If we consider the easiness for users, it would be easier to swipe a finger on the screen to unlock the device rather than typing a strong and difficult password or drawing a complicated pattern to authenticate the device frequently.

In a study on users′ point of view about authentication, Furnell et. al.[17, 18] demonstrated that users are looking for solutions which are not only comfortable for repetitive use but also provide a strong security mechanism for the device, so that the users could enjoy the free benefits of the advanced functionalities of smart devices without worrying about security. The study discovers that users are more interested in the use of biometrics and physical characteristics of an individual rather than the visual techniques of authentication that are based on the knowledge of the users[18], like passcode, PIN, password, security code etc. Another survey was conducted in the Kingdom of Saudi Arabia[6] in which the authors indicated the dissatisfaction of the mobile phone users about the security of the data in their smart devices; emphasising that users need some powerful authentication and that again biometric authentication is the most preferred among the users. Almost all of these studies and surveys are limited to some specific places of the globe.

There are different techniques implemented in smart phones for secure user identification, and many of them are under progress for improvement and implementation. Authentication mechanisms commonly used in smart devices are discussed below:

1) Password/PIN/Security code/Passcode: The first authentication mechanism introduced in the cellular phones was based on security code, a string that user enters to unlock phone. The same method has also been implemented for authorized access of smart devices. This security mechanism is based on memorizing a string that user has to enter in order to access personal device. A number of different schemes are employed for the strength of security code based authentication in smart devices like the number of characters, digital or alphanumeric, timeout after a few incorrect attempts, etc.

The personal identification number (PIN) is a secret-knowledge[6] authentication method and therefore is dependent on information possessed by the authorized user, i.e., what the user remembers or knows. In iOS smart devices, the term passcode is used as a digital lock limited to 4 digits, whereas in android phones PIN can be from 4 to 16 numeric digits.

PIN and passwords are perceived as the same by most of the users, but in technical smartphone terms these are different in the aspect that PIN is based on numeric digits whereas password can contain alphanumeric and special characters as well. In Android phones, a password must be at least 4 characters but no longer than 16 characters. Although the PIN and password are the most commonly used methods for authentication in information systems, such secret-knowledge approaches unfortunately have traditional problems, and most of the times the exposure of the knowledge is done by the authorised individuals themselves[6] or a shoulder-surfer might be able to steal the password typed in by the user. Even with a lot of troubles and inconvenience, the password authentication technique is dominant among all for access control in smart devices[7]. In the smart devices, the most well-liked password or passcode authentication technique is a 4-digit lock[15], and in this form of authentication, users select 4-digits of their choice in a definite sequence and set as the passcode of their devices. Users are then required to enter these 4 digits in exactly the same sequence to unlock the device. So, in this approach, there can be any one combination of at least 4 digits out of at least 10 000 combinations. Many devices support the PIN of more than 4 digits (but less than 16 digits). In the same manner, a password can be set by a user to secure the personal device, but it is a bit complicated because it contains digits, alphabets as well as special characters.

The PIN/Password security was simplified from long

and complicated security codes to a pure-digit[19] passcode. This 4-digit PIN code could have about 10 000 combinations. This technique has been now improved to 5-digit code lock, which is more difficult to break because of the increased number of combinations.

2) Pattern lock: A substitute of password authentication technique has been introduced in Android operating system in smart devices in the form of pattern lock; and it is now the most common among the android users[20]. Users are allowed to select a pattern by connecting four or more dots from nine, a 3×3 grid as shown in Fig. 1 (a). Each circle or dot can be passed by only once in the selected pattern[15, 19]. The connected dots/circles then form a unique pattern that can be used to unlock the smart device. The pattern lock is not considered as reliable by some people because it leaves some oily smudges[21] of finger on the smart screen, by which it is sometimes easily guessable[22, 23], but it is not likely to occur every time and in every case. Also, if the entered pattern lock is correct, the green colour of pattern is quite visible for a distant attacker; otherwise, if wrong, it is marked as red, and disappears in 1 or 2 seconds. However, from the security perspective, this mechanism has been strengthened in Android by making the pattern invisible if it is correct, thus preventing shoulder surfing[21].

3) Email ID/Password: Most of smart phones store user′s Email ID and password, which can be used in online authentication process or to download applications from the authenticated online store. It depends on the operating system of the smart phone[24]. In the context of authentication of the smart device, usually the user is asked for his stored email ID and password when he enters the wrong passcode or pattern three to five times (as shown in Fig. 1 (b)). This technique is more common in Android.

4) Biometrics: Nowadays biometric authentication is becoming very popular as an alternative to other knowledge-based authentication schemes. Biometrics, as a novel authentication mechanism in smart devices can be physiological or behavioural[20]. However, the most common among smart devices so far is the physiological biometric.

5) Physiological biometrics: Physiological biometric is based on the physical characteristics of an individual, like fingerprint, iris, face, voice and retina. The benefits and limitations of novel physiological biometrics has been summarized in Table 2 below.

Fingerprint is a famous authentication technique which was first introduced in smart devices by iOS as touch ID with the launch of iPhone 5S[28, 29]. In iPhone 5S, there is installed a fingerprint scanner in the homes-screen button. When the user presses the home-screen button, the device automatically scans the finger and grants access to the authorized user without typing in the PINs or passwords. With the implementation of this approach, Apple already declared that fingerprint scanner was not much trustworthy[30]. The same technique was followed by Android in HTC One Max[31], where the fingerprint sensor has been put at the back of the phone. Samsung Galaxy S5 has used the Apple′s approach and placed the fingerprint sensor in the home button[32]. This feature is expected to be available in many upcoming smart devices.

Face detection has also become a common biometric authentication among smart devices in the recent years. Android launched its first smart device with a facial recognition mechanism to unlock the device in late 2011, which later on was employed by Apple′s iPhone 5S[28]. Facial recognition is considered as less secure because it can be spoofed by placing authenticated user′s photo in front of the camera. However, to minimize the risk, some of the devices have implemented the technique of eye blinking before the device is unlocked. In some Android devices, face lock is combined with voice recognition in order to enhance user

Table 2 Benefits and limitations of biometric authentication for smart phones

Method	Benefits	Limitations	Examples
Fingerprint authentication	Unique to individuals. Easily unlocks the phone by swiping a finger. It also enables the users for online transactions by fingerprint verification via smart phone.	Smart phones with built-in fingerprint reader are limited in number. Needs integration with network access software. Requires extra hardware fingerprint reader/sensor.	iPhone 5s, HTC One Max, Pantech Vega LTE-A, Samsung Galaxy S5.
Facial/Ear recognition, Iris/Retinal scanning	Easy to use. Do not require any extra hardware. Many applications are available for this authentication method.	Cannot be used in low light environments. Iris[25]/Retinal scanning is not currently available to common users, however some applications and tools have been developed to support eyeverification in smart devices[26]. Facial recognition is said to be easily cheated by a picture of the actual owner.	Samsung Galaxy Nexus, Visidon AppLock tool for Android. AOptix, an application for iPhone to scan iris. Ergo is an application that supports ear lockscreen technology[27].
Voice recognition	No extra hardware required, since microphone is already available in every phone.	Voice changes with the age, or because of a throat infection. Difficult to use in environments like in a meeting or in a classroom.	Nuance mobile VocalPassword, Samsung Galaxy S III, Apple iPhone 4s, and numerous voice recognition applications.

authentication. However, Android declares the face-lock and face-and-voice-lock combined as less secure than a pattern, PIN or password, and a person who looks similar to the user can unlock the phone[28]. With biometric authentication, smart devices also allow users to keep a PIN or a password as a backup for accessing the device, in case of not being able to unlock the device by biometric authentication like face or fingerprint.

Researchers consider iris and retina scanning as the next level of security in smart devices. According to the studies, they are neither easy to implement nor comfortable for a user to access the personal device repeatedly. AOptix has developed a tool that lets iPhone 4 users to scan iris[26]. Both iris and retina scanning would need a camera with infrared light and installing such sensors in a mobile device could be hard. Also, iris and retina scanning requires users to be closer to the device, which can be annoying if they have to do it on a regular basis.

Other than fingerprint, face, voice and eye verification, ear biometric recognition is also being introduced in Android smart devices using an application from Google store[26]. Many other technologies are being developed and introduced to support ear biometric in smart devices as a lock screen technology[27, 33].

6) Behavioural biometrics: The behavioural biometric is based on the behaviour of the individual like user′s gait, habitual and location information, keystroke patterns, signature and gesture based identification. Shi et al.[34] proposed the use of behavioural biometrics as an alternative for passwords and knowledge-based authentication; and their authentication system is based on multiple cues such as location information or communication. The behavior-based authentication techniques work by analyzing user behavior of holding the device, keystroke dynamics, touchscreen patterns, etc. All such analysis requires the basic sensors which are already present in a smart device like accelerometer and touch sensors, and usually no extra hardware is required to implement behavioural biometrics.

The signature recognition is based on the way a user makes signature by length and number of strokes and acceleration, rather than comparing with the original signature.

Rhythm-based locking system (RLS)[35] is similar to the keystroke dynamics based on user′s habits and skills. Some researchers used virtual keyboards to inspect this authentication technique in smart devices[36].

In addition to the above described authentication techniques, gesture-based authentication is being worked upon by researchers, like gait and other human body gestures using the accelerometer or gyroscope which is available in all touch-screen smart devices[37, 38]. This technique works by tracing user′s walking patterns and different poses like hand gestures[39].

Moreover, applications are being developed to measure user behavior, e.g., ECG (Electrocardiogram). Cardiograph is an Android application which measures heart rate. The application uses device′s built-in camera, light-emitting diode (LED) or a specific sensor to calculate and plot user′s ECG[40, 41]. Although such applications have been in use for health and fitness purposes, in the near future they can be used to enhance authentication.

7) Multimodal authentication: Multimodal authentication is based on using more than one (upto three) authentication mechanisms to protect user privacy and confidential data in a personal device. Similarly, multimodal-biometric authentication employs two or more biometrics to authenticate users of smart devices. It is considered to give high performance and measurability when applied in smart devices[42] and reduces the risk of fraud as compared to unimodal authentication[41, 43]. Also, it provides users with more confidentiality to protect high profile data in smart devices.

Additionally, some sensitive tasks of the smart devices, like online banking transactions, require multiple authentications. For example, some business and financial services add another layer of user authentication by sending a code via email and sending another password by SMS before a user completes the transaction[44]. This is beneficial to confirm the authorization of the authenticated user and avoid fraudulent transactions.

3 Comparative analysis

For the evaluation of preferred authentication mechanisms among the smart device users and their opinion about the private and confidential data security, a survey was conducted. The statistical analysis of different survey questions is discussed below.

1) Survey data collection: We distributed about 400 questionnaires online and offline, out of which 320 interestingly participated in the survey. We intended to target the participants from all age groups without gender discrimination. As a result, most of the responses were from people of 21 to 30 years of age, among whom the smart devices are currently more popular.

2) Tools used: The data collected was compiled using MS access and MS Excel, and statistical package for social sciences (SPSS statistics v20) was used to accomplish the statistical analysis of the questionnaires.

3) Survey questions: The questionnaire comprises of different questions to analyse the perception of common users about security risks, threats and authentication mechanisms.

This paper will only discuss those questions which are related to the evaluation of the authentication techniques of the smart devices and check the users′ preference and confidence levels for different authentication techniques implemented so far in the smart devices.

1) Respondents diversification: The responses were diversified from certain different places over the globe; and to track this, respondents were asked about their location. Table 3 shows the diversification of the participants. Most of the participants, 250, were from Pakistan, 36 from USA, 1 from Australia, 1 from Germany, 1 from Nigeria, 1 from Palestine, 1 from Turkey, 1 from Denmark, 2 from France,

2 from India, 2 from Canada, 2 from KSA, 3 from UAE and 17 from UK.

Table 3 Area-wise distribution of participants

Place/Country	Number of respondents
Australia/Denmark/France	4
Germany/Nigeria/UK	19
Pakistan/India	252
Palestine/Turkey/UAE/KSA	7
USA/Canada	38
Grand total	320

2) Gender and age-group: In the questionnaire, after location, respondents were then asked about their gender and age. The gender and age based distribution of participants and the numeric values obtained from the results have been plotted in Fig. 2 below.

It can be seen that 14.38% of the participants belong to 15-20 year-old category; the maximum 45.31% of the participants are from the 21-25 year-old category; 25% are from 26-30; 7.81% are from 31-35 and 7.50% are from greater than 35 years old.

3) Smart device′s type, manufacturer and operating system: It is also important to consider which device is used by the user and which is the most popular manufacturer and operating system among the users who participated in this survey. For this purpose, a question was included in the questionnaire that asked about the smart device that the respondent uses, followed by a question about its manufacturer and operating system. The frequency of this is shown in Table 4 below.

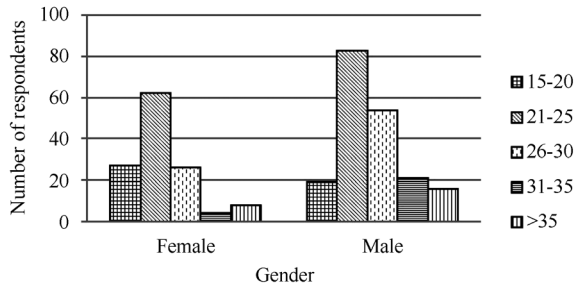


Fig. 2 Age and gender-wise distribution of participants

As shown in the table, most of the received data is from the 262 smart phone users, 26 use iPad, 13 use Tablet, 4 use Phablet, 4 use Note and 11 are on others. As to manufacturers of smart devices, leading are Apple and Samsung with 84 and 79 respondents respectively, 47 have Nokia, 35 have HTC, 35 have QMobile, 17 have Blackberry, 23 have smart devices from other manufacturers. Similarly, the most popular operating system is Android, which agrees with the rapidly increased number of smart phone users, especially the number of Android users[19, 45]. The second in number is iOS, and 84 of our respondents use it.

4) Private data in smart device: A smart device contains the owner′s personal data like emails, text messages, contact lists, photos etc. Some of the users also use their smart devices for security sensitive tasks like online banking[46]. When the respondents were asked whether they have got some private data in their smart devices or not (though it is most likely that every user will have some private data in the smart device they use), about 14% of the respondents said that they do not have any private data in their smart device, whereas 86% agreed that they definitely have got private and confidential data in their smart devices, as shown from the analysis in Fig. 3.

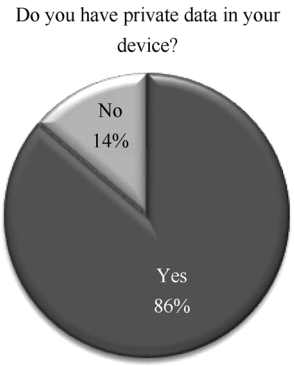


Fig. 3 Responses for storing private stuff in the smart device

In the survey questionnaire, respondents were given different options and asked about which data in their smart devices is private or confidential. In users′ opinion, private data can be Gallery/Photos (73%), Messages (64%), Contacts (59%), Personal information (51%), Emails (47%), Social networks (40%), Call logs (27%), Addresses (27%),

Table 4 Smart device, manufacturer of device and operating system used by respondents

Smart device	Total number of respondents	Manufacturer	Total number of respondents	OS	Total number of respondents
IPad	26	Apple	84	Android	154
Note	4	Blackberry/RIM	17	Blackberry OS	18
Other	11	HTC	35	iOS	84
Phablet	4	Nokia	47	java	4
Smart phone	262	Other	23	Other	6
Tablet	13	QMobile	35	Symbian	21
		Samsung	79	Windows	33

Appointments (14%), Birthdays (12%), and Other (4%), as shown in Table 5.

5) Importance/sensitiveness of data: The questionnaire also asked users to rank importance/sensitiveness of data on smart phones. In response to this, users rated the importance/sensitiveness of data on their devices as Very High (32.5%), High (39.7%), Moderate (23.1%), Low (3.8%), and Very Low (0.9%), as shown in Table 6 below.

Table 5 Private data in users′ opinion

Data	Total % of respondents
Gallery/Photos	73%
Messages	64%
Contacts	59%
Personal information	51%
Emails	47%
Social networks	40%
Call log	27%
Addresses	27%
Appointments	14%
Birthdays	12%
Other	4%

6) Required level of protection: The next statistics, about the level of protection they require for data in a personal device, show that users want a Very High level of protection for their device i.e., 45.6% respondents, High (338.1%), Moderate (13.4%), Low (1.6%) and Very Low (1.3%).

7) Used authentication mechanism and confidence level: Fig. 4 shows the results of responses to the specific security questions about which authentication technique respondents use and how much confident they are in using this technique.

It is found when figured out of the total that still 52.8% respondents use PIN/Security code authentication technique and about 30.31% use the modern Pattern authentication mechanism. Results show that only 5.63% respondents use biometrics authentication, which can be inferred from the fact that biometrics security is currently not very common among the smart devices of ordinary users.

The statistics also show that still most of the people (25% out of the 320 respondents) are satisfied and about 25% are on the average while using PIN/Security code like Password as the authentication mechanism. Similarly, since pattern authentication is a new technology, about 13.13% are satisfied, and 14.7% are neither satisfied nor dissatisfied.

8) Knowledge-based authentication: The survey included some specific questions about knowledge-based authentication techniques. For those who use Password/PIN security (82.81%), most of them think that it is not difficult to remember passwords (55.63%) as shown in analysis in Table 7. We can infer that most of the people are still willing to use passwords and they have no difficulty with remembering passwords. Passwords can be shared and forgotten, which can cause the breach of authentication. In response to this 45.94% of respondents said that they

Table 6 Private and confidential data in smart devices

Rate the importance/sensitiveness of your data on your smart phone	Total number of respondents	What level of protection you require for your data on the device?	Total number of respondents
Very High	104 (32.5%)	Very High	146 (45.6%)
High	127 (39.7%)	High	122 (38.1%)
Moderate	74 (23.1%)	Moderate	43 (13.4%)
Low	12 (3.8%)	Low	5 (1.6%)
Very Low	3 (0.9%)	Very Low	4 (1.3%)

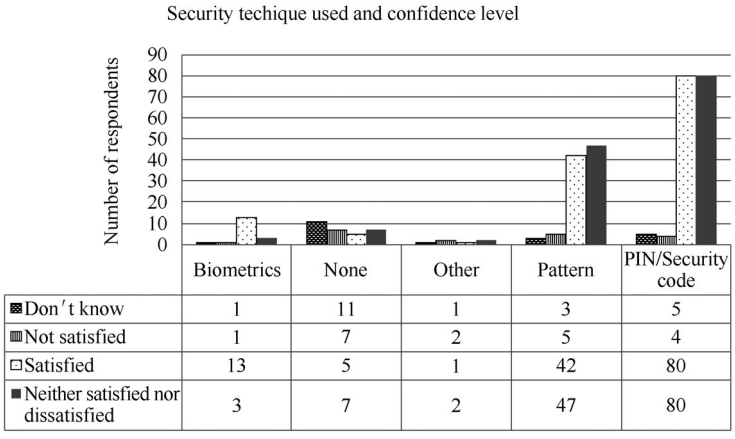


Fig. 4 Security technique used and confidence level of respondents

forgot or shared their passwords, while 54.06% disagreed with this. The survey results are somewhat likely to the statement by Clark et al. that the users are not only aware of the weaknesses of PIN/Password authentication but also much concerned about the exposure of their credentials to others[23].

9) Biometric authentication: A few questions were dedicated to the biometric authentication in the smart device and how users perceive this innovative authentication mechanism as compared to traditional authentication techniques. About the biometric security authentication mechanism, many of the people were unaware of it, and very few (19.38%) have ever used some biometric authentication technique (Table 8). This is perhaps due to the reason that biometrics are still not very common among the ordinary users.

About the reliability of the biometric authentication, the majority of the respondents (61.88%) think that biometric security is a secure and reliable authentication technique for the smart devices (Table 8). However, 28.75% of the respondents do not know whether the biometric authentication is much more reliable or not, which means that many people do not know much about biometrics.

10) Preferred authentication mechanism: At the end, the survey questionnaire asked the respondents about their preference among all the authentication techniques including biometric.

The evaluation on all the authentication techniques shows that most preferred authentication techniques among the users seem to be Biometric authentication[47] (54%) and PIN/Password (27%), as shown by Table 9 and Fig. 5, whereas 14% prefer Patterns because visual representations are more memorable and easier to recall[48].

11) Preferred biometric authentication mechanism: Specifically for the biometric security authentication, the survey concluded by asking the respondents that if they are only allowed to use biometric authentication, which one biometric they would choose for their smart devices (Fig. 6).

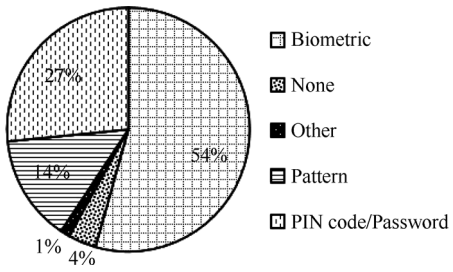


Fig. 5 Preferred authentication mechanism

Table 7 PIN/Password authentication

Have you ever used PIN/Password security for your device?	Is it difficult to remember?		Have you ever forgotten or shared?		Total
	Yes	No	Yes	No	
Yes	27.19%	55.63%	40.94%	41.88%	82.81%
No	6.25%	10.94%	5.00%	12.19%	17.19%
Total	33.44%	66.56%	45.94%	54.06%	100.00%

Table 8 Biometric authentication usage: reliable or not

Biometric authentication usage	Reliable or not	Total % of respondents
Have you ever used any of the biometric authentication techniques?	Yes	19.38%
	No	80.63%
Do you think that biometric security is more secure and reliable?	Yes	61.88%
	No	9.38%
	Don′t know	28.75%

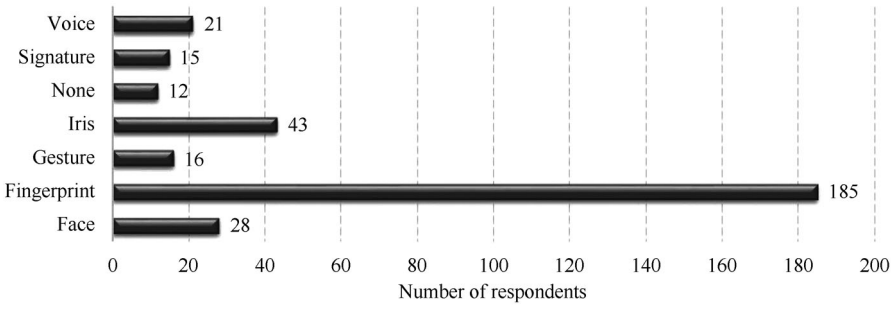


Fig. 6 Biometric authentication and number of respondents

Table 9 Preferred authentication mechanism

Which technique would you prefer for the authentication of your smart device?	Total number of respondents
Biometric	174
None	12
Other	4
Pattern	45
PIN code/Password	85

The most preferred among the users is fingerprint[47] (57.81%), probably because of the fact that it is easily available in most of the smart devices and the latest smart phones. Iris is secondly preferred by 13.44% of the respondents (Table 10).

Table 10 Biometric authentication

Preferred biometric	Total % of respondents
Face	8.75%
Fingerprint	57.81%
Gesture	5.00%
Iris	13.44%
None	3.75%
Signature	4.69%
Voice	6.56%

Majority of the respondents′ concern for the biometric authentication techniques shows that this will be more preferred among the users in the near future when available commonly in all devices. Since, it is more convenient to just place your finger on the sensor or just have a look (Iris) at the device to unlock than to type a whole phrase of difficult password.

4 Summary and recommendations

There are certain facts, related to authentication mechanisms in smart devices in the present world, those have been revealed as a result of this survey and research as categorized and discussed below.

1) Preference for visual-based authentication: According to the survey results, the percentages of respondents using each authentication technique are shown in Table 11. The results indicate that about 52.81% of total respondents use PIN/Security code for the authentication of their smart device; 30.31% of respondents use pattern recognition; and only 5.63% of respondents are using biometrics. It can be inferred from the analysis that still most of the people prefer PIN/Security code and patterns for authentication despite the fact that they are difficult to memorise and impractical for frequent use[19].

From the security and privacy perspective, iOS provides the option of data wipe after 10 incorrect passcode entries. Android locks the phone after a number of incorrect PIN or password entries but leaves the option of getting back using Google password, otherwise a factory reset is needed that wipes off all the data from the device. This is one of the reasons that smart phone users compromise the security of data by using convenient and easy-to-hack passwords.

Table 11 Percentages of respondents using each authentication technique

Authentication technique used	Total % of respondents
PIN/Security code	52.81%
Pattern	30.31%
Biometrics	5.63%
Other	1.88%
None	9.38%

The 3×3 grid visual-based pattern lock is also common among the smart device users. Although it provides an easy mechanism for touch-dragging, the security level could be weak if the user enters an easy pattern for convenience or it can be uncomfortable for frequent use if a complicated pattern is entered[45].

2) Cost of biometric-based smart devices and preference for biometric authentication: Although users are very much concerned about the privacy in their smart devices and look for better options to protect the private and confidential data, most of them are unable to use the latest authentication techniques because of the unavailability of latest devices at affordable prices, especially in the developed countries like Pakistan, and therefore they are inclined to use the traditional and visual-based authentication mechanisms.

The lower percentage of respondents using biometrics shows that biometric authentication is currently not quite common and popular perhaps due to reasons like many people are unaware of the biometric authentication scheme or the relatively high cost of high-end mobile phones with this feature. Also, in developed countries like Pakistan, smart devices with biometrics enabled authentication are not in range of an average salaried man. Furthermore, when respondents were asked about the preference of an authentication mechanism, the highest percentage is in favor of biometric authentication, which means that people believe that biometrics can provide far better security than traditional visual based authentication mechanisms. Out of different biometrics, people usually prefer fingerprint authentication because it is convenient to use with some popular smartphone models that provide this utility. Face and Iris recognition are not much preferable among the smart phone users.

The physiological biometric based authentications (like fingerprint, Iris, etc.) mostly require an additional hardware which may not be commonly available in smart phones so far[49, 50]. For the biometric identifiers, technically the device scans the physical characteristic and stores it as a string of data. When the user tries to authenticate the device next time, the two data strings are compared, and the user is authenticated if sufficient similarity is achieved. Despite of the popularity among the smart phone users and common perception of better and advanced security, the

biometrics can easily be faked. For example, fingerprint can be captured on sticky tape and a fake gelatine copy can be generated. Similarly photos of eye retina can be presented to dodge authentication. However, for the users′ easiness, convenience and security, some smart phone companies like Samsung now offer authentication not only to unlock the device but also for some online banking and to secure folders on the phone. Moreover, for the phones lacking hardware for biometric authentication, devices and modules are being introduced in the market to enable secure biometric authentication. For example, iFMID SIC Snap-on[51] is the fingerprint reader module made for iPhone. This offers a secure biometric authentication mechanism with single sign-in to mobile confidential data and applications.

3) Behavioural and Multi-factor Authentication: The emerging authentication mechanism in the recent past include behavioural biometric authentication which is based on human actions like keystroke dynamics[52], gestures and features[53]. This technique is prospering in literature for authenticating smart phone users through numerous machine learning classifiers[49]. Another recent method in the smart phone security is multi-factor authentication mechanism[54], which combines traditional authentication factors, including something the user has (e.g., a card), something the user knows (e.g., passcode) and something the user is (e.g., fingerprint)[55]. It can be viewed like user will be first asked for fingerprint and then for the password to fully authenticate the smart device[56]. In addition to that, another scheme for authentication is currently in progress based on re-authentication mechanism[57]. The advantage of this scheme is that the device provides a continuous protection. When a user leaves the unlocked smart phone at some place, it is very easy for an attacker to access that, even if the smart device is locked, the attacker can bypass screen lock using operating system flaws that may exist in Android and iOS[57]. Thus, in such a scenario a re-authentication technique is helpful in protecting user′s privacy.

4) Impact of cultural habits and confidentiality breach: The adoption of authentication technique for smart devices and for certain applications varies according to the cultural aspects of a region. For example, confidentiality breach of a common man′s address book in his phone may contain only friends and family numbers that do not have much impact if disclosed to someone whereas, if certain employees of an organization face confidentiality breach, it can reveal important business contacts, customer relations and secret codes. In a developed country like Pakistan, there is no existence of law for confidentiality breach, so people feel free to use someone else′s phone if left unattended. Such confidentiality breaches can disrupt the company services or an individual′s life.

5) Interest in new technology: There are numerous research work going on in the field of smart phone authentication techniques and every other day smart phone manufacturers are releasing new handsets with innovative and improved authentication mechanisms but still users are demanding higher, demanding more and at a cheaper price. The fact is that most of the users stay updated to the latest innovation in the smart phone world but they remain unable to adopt it due to very high cost.

6) Different assumptions of private data by different users: It could be clearly observed from the survey results that the more smart phone users are conscious about their private data such as photos, messages, contacts, personal information and, most importantly, bank account information with the introduction of mobile banking in smart phones, the more is the need for stronger authentication mechanisms. This perception of private data varies among the users with age, region and also by profession. For example, a common user will consider his contacts and family photos as sensitive data whereas, for a businessman, business contacts and transactions via mobile apps are the most sensitive data.

Most of the smart phone users are still using and are comfortable with the PIN/Security code authentication mechanism which is no doubt a strong authentication technique although there is a chance of forgetfulness and failure in using PIN/Security code. On one side, the security codes and passwords should be strong enough to make them unbreakable and on the other side easy enough to remember without disclosing and writing somewhere for remembrance.

Moreover, the research work infers that the biometric security provides a stronger authentication mechanism than any of the knowledge based authentication schemes. One major reason is because biometrics authenticate what the user is claiming instead of what the user remembers and hence are difficult to deceive. The biometric authentication is highly recommended for the users who want more security for their private data in smart devices. Also, additional biometric authentication modules like camera for iris or face scanning and fingerprint modules in smart devices need to be enhanced to reject fake authentication attempts.

7) Biometrics - A step towards modernization of authentication: The overall smartphone security very much relies on authentication techniques due to increased ratio of loss and theft of smart phones and devices[5]. Although there are numerous modern and up-to-date authentication modes and types, still users want stronger and durable authentication for their smart devices.

Based on analysis and findings of this research, most of the users believe that biometric authentication is reliable enough to fulfil their security requirements. Biometric authentication mechanisms are not only limited to physical characteristics of an individual, like fingerprint, iris, ear, voice, retina, palm and face but the latest trends of biometric authentication also include the behavioural aspects of an individual like gait, gesture, signature, keystroke patterns, electro cardiogram (ECG), electro encephalogram (EEG) and many more.

However, most of the modern biometrics are not available to common users, as mostly latest models (which must be expensive) of smart devices and applications are equipped with fingerprint sensor, ear-based authentication,

facial and voice recognition tools. Iris scanning is also available via AOptix, an application and biometric scanning tool for iPhone. According to the survey analysis, biometric authentication mechanisms, if easily available to common users, will be widely used, accessed, preferred and will become more secure authentication schemes in the near future.

5 Conclusions

In the present world, smart devices are getting smaller and handy. All the data and activities that used to be on personal and desktop computers are rapidly being transferred to handheld smart devices. Since smart devices have become more functional and may carry a large amount of owner′s private and confidential data with the risks of theft or getting lost; there must be some reliable and efficient techniques for authentication so that users feel more confident about using their smart devices for personal and confidential tasks.

The results of this paper show that users are still looking for further enhancements in the authentication mechanisms of smart devices to make them practically more usable and operational. Moreover, the biometric technique is more reliable than any of traditional authentication mechanisms and can efficiently meet the users′ need. Also, the input sensors in smart devices, like cameras, microphones, touch screens and GPS[58], make the implementation and embedding of biometrics in smart devices much easier[59]. The survey results presented in this paper also expose a number of facts related to smart devices′ security and authentication such as the most popular smart phone operating system among users, types of data stored in users′ smart devices, user-preferred techniques for authentication of device and protection of data, and the preferable biometrics among users for the authentication of smart phones. The fear of loss and exposure of confidential data can be a hindrance in the adoption of advancements in smart devices′ technologies for multiple tasks and functions.

Authentication schemes for smart phones are evolving day by day. In future the innovations for smart phone authentications shall be evaluated based on users experience and preference for what can be done to further improve the authentication mechanisms to protect users′ privacy in the light of fast growing security threats.

References

[1] K. Zhang, X. H. Liang, X. M. Shen, R. X. Lu. Exploiting multimedia services in mobile social networks from security and privacy perspectives. *IEEE Communications Magazine*, vol. 52, no. 3, pp. 58–65, 2014.

[2] I. Muslukhov, Y. Boshmaf, C. Kuo, J. Lester, K. Beznosov. Understanding users′ requirements for data protection in smartphones. In *Proceedings of the 28th International Conference on Data Engineering Workshops*, IEEE, Arlington, USA, pp. 228–235, 2012.

[3] M. La Polla, F. Martinelli, D. Sgandurra. A survey on security for mobile devices. *IEEE Communications Surveys and Tutorials*, vol. 15, no. 1, pp. 446–471, 2013.

[4] D. Ghosh, A. Joshi, T. Finin, P. Jagtap. Privacy control in smart phones using semantically rich reasoning and context modeling. In *Proceedings of 2012 IEEE Symposium on Security and Privacy Workshops*, IEEE, San Francisco, USA, pp. 82–85, 2012.

[5] N. L. Clarke, S. M. Furnell. Authentication of users on mobile telephones-A survey of attitudes and practices. *Computers & Security*, vol. 24, no. 7, pp. 519–527, 2005.

[6] T. Alhussain, R. AlGhamdi, S. Alkhalaf, O. Alfarraj. Users′ perceptions of mobile phone security: A survey study in the Kingdom of Saudi Arabia. *International Journal of Computer Theory and Engineering*, vol. 5, no. 5, pp. 793–796, 2013.

[7] C. Herley, P. C. Van Oorschot, A. S. Patrick. Passwords: If we′re so smart, why are we still using them?. In *Proceedings of the 13th International Conference, Lecture Notes in Computer Science*, Springer, Accra Beach, Barbados, vol. 5628, pp. 230–237, 2009.

[8] N. Ben-Asher, N. Kirschnick, H. Sieger, J. Meyer, A. Ben-Oved, S. Mller, S. On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, ACM, New York, USA, pp. 465–473, 2011.

[9] A. Jain, R. Bolle, S. Pankanti. Introduction to biometrics. *Biometrics*, A. Jain, R. Bolle, S. Pankanti, Eds., USA: Springer, pp. 1–41, 1996.

[10] A. Pocovnicu. Biometric security for cell phones. *Informatica Economică*, vol. 13, no. 1, pp. 57–63, 2009.

[11] M. Tamviruzzaman, S. I. Ahamed, C. S. Hasan, O. Casey. ePet: When cellular phone learns to recognize its owner. In *Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration*, ACM, New York, USA, pp. 13–17, 2009.

[12] I. Muslukhov. Survey: Data protection in smartphones against physical threats. *Term Project Papers on Mobile Security*, The University of British Columbia, Canada, 2012.

[13] M. Theoharidou, A. Mylonas, D. Gritzalis. A risk assessment method for smartphones. In *Proceedings of the 27th IFIP TC 11 Information Security and Privacy Conference*, Springer, Heraklion, Greece, vol. 376, pp. 443–456, 2012.

[14] T. Dorflinger, A. Voth, J. Kramer, R. Fromm. My smartphone is a safe! The user′s point of view regarding novel authentication methods and gradual security levels on smartphones. In *Proceedings of the 2010 International Conference on Security and Cryptography*, IEEE, Athens, Greece, pp. 1–10, 2010.

[15] A. Arif, M. Pahud, K. Hinckley, W. Buxton. A tap and gesture hybrid method for authenticating smartphone users.

In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, ACM, New York, USA, pp. 486–491, 2013.

[16] M. Meints, H. Biermann, M. Bromba, C. Busch, G. Hornung, G. Quiring-Kock. Biometric systems and data protection legislation in Germany. In *Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, IEEE, Harbin, China, pp. 1088–1093, 2008.

[17] S. Furnell, N. Clarke, S. Karatzouni. Beyond the PIN: Enhancing user authentication for mobile devices. *Computer Fraud and Security*, vol. 2008, no. 8, pp. 12–17, 2008.

[18] M. Jakobsson, E. Shi, P. Golle, R. Chow. Implicit authentication for mobile devices. In *Proceedings of the 4th USENIX Conference on Hot Topics in Security*, USENIX Association, Berkeley, USA, pp. 9, 2009.

[19] L. F. Wu, X. J. Du, X. W. Fu. Security threats to mobile multimedia applications: Camera-based attacks on mobile phones. *IEEE Communications Magazine*, vol. 52, no. 3, pp. 80–87, 2014.

[20] A. De Luca, A. Hang, F. Brudy, C. Lindner, H. Hussmann. Touch me once and I know it′s you!: Implicit authentication based on touch screen patterns. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Austin, USA, pp. 987–996, 2012.

[21] A. De Luca, M. Harbach, E. Von Zezschwitz, M. E. Maurer, B. E. Slawik, H. Hussmann, M. Smith. Now you see me, now you don′t: Protecting smartphone authentication from shoulder surfers. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, New York, USA, pp. 2937–2946, 2014.

[22] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, J. M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, USENIX Association, Berkeley, USA, 2010.

[23] A. De Luca, E. Von Zezschwitz, N. D. H. Nguyen, M. E. Maurer, E. Rubegni, M. P. Scipioni, M. Langheinrich. Back-of-device authentication on smartphones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, New York, USA, pp. 2389-2398, 2013.

[24] W. Jeon, J. Kim, Y. Lee, D. Won. A practical analysis of smartphone security. In *Proceedings of the Symposium on Human Interface 2011, Lecture Notes in Computer Science*, Springer, Orlando, USA, vol. 6771, pp. 311–320, 2011.

[25] M. Qi, Y. H. Lu, J. S. Li, X. L. Li, J. Kong. User-specific iris authentication based on feature selection. In *Proceedings of the 2008 International Conference on Computer Science and Software Engineering*, IEEE, Wuhan, China, vol. 1, pp. 1040–1043, 2008.

[26] A. Goode. Bring your own finger-how mobile is bringing biometrics to consumers. *Biometric Technology Today*, vol. 2014, no. 5, pp. 5–9, 2014.

[27] Descartes Biometrics. ERGO ear biometric app: Unlock your phone with your ear, [Online], Available: http://www.descartesbiometrics.com/ergo-app/, February 10, 2015.

[28] S. Furnell, N. Clarke. Biometrics: Making the mainstream. *Biometric Technology Today*, vol. 2014, no. 1, pp. 5–9, 2014.

[29] Apple-iPhone-Compare models, [Online], Available: http://www.apple.com/iphone/compare/, February 10, 2015.

[30] M. Campbell. Apple further details new Touch ID fingerprint sensor, notes system is not flawless. September 11, 2013, [Online], Available: http://appleinsider.com/articles/13/09/11/apple-further-details-new-touch-id-fingerprint-sensor-notes-system-is-not-flawless, February 11, 2015.

[31] HTC one max-about the fingerprint scanner, [Online], Available: http://www.htc.com/us/support/htc-one-max/howto/445037.html, February 10, 2015.

[32] Samsung GALAXY S5, [Online], Available: http://www.samsung. com/global/ microsite/ galaxys5/ features. html, February 11, 2015.

[33] P. N. A. Fahmi, E. Kodirov, D. J. Choi, G. S. Lee, A. Mohd Fikri Azli, S. Sayeed. Implicit authentication based on ear shape biometrics using smartphone camera during a call. In *Proceedings of International Conference on Systems, Man, and Cybernetics*, IEEE, Seoul, South Korea, pp. 2272–2276, 2012.

[34] E. Shi, Y. Niu, M. Jakobsson, R. Chow. Implicit authentication through learning user behavior. In *Proceedings of the 13th International Conference, Lecture Notes in Computer Science*, Springer, Boca Raton, USA, vol. 6531, pp. 99–113, 2011.

[35] J. D. Lee, Y. S. Jeong, J. H. Park. A rhythm-based authentication scheme for smart media devices. *The Scientific World Journal*, vol. 2014, pp. 781014, 2014.

[36] F. D. Li, N. Clarke, M. Papadaki, P. Dowland. Active authentication for mobile devices utilising behaviour profiling. *International Journal of Information Security*, vol. 13, no. 3, pp. 229–244, 2014.

[37] D. Gafurov, K. Helkala, T. Sndrol. Biometric gait authentication using accelerometer sensor. *Journal of Computers*, vol. 1, no. 7, pp. 51–59, 2006.

[38] T. Hoang, D. Choi. Secure and privacy enhanced gait authentication on smart phone. *The Scientific World Journal*, vol. 2014, pp. 438254, 2014.

[39] C. S. Koong, T. I. Yang, C. C. Tseng. A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal*, vol. 2014, pp. 781234, 2014.

[40] Cardiograph, [Online], Available: https://play.google.com/store/apps/detailsid = com. macropinch. hydra. android&hl=en, February 11, 2015.

[41] Y. D. Lin, H. Y. Ho, C. C. Tsai, S. F. Wang, K. P. Lin, H. H. Chang. Simultaneous heartbeat and respiration monitoring using PPG and RIIV on a smartphone device. *Biomedical Engineering: Applications, Basis and Communications*, vol. 25, no. 4, Article number 1350041, 2013.

[42] P. S. Sanjekar, J. B. Patil. An overview of multimodal biometrics. *Signal & Image Processing: An International Journal*, vol. 4, no. 1, pp. 57–64, 2013.

[43] H. Aronowitz, M. Li, O. Toledo-Ronen, S. Harary, A. Geva, S. Ben-David, A. Rendel, R. Hoory, N. Ratha, S. Pankanti, D. Nahamoo. Multi-modal biometrics for mobile authentication. In *Proceedings of the 2014 IEEE International Joint Conference on Biometrics*, IEEE, Clearwater, USA, pp. 1–8, 2014.

[44] P. Ruggiero, J. Foote. Cyber threats to mobile phones. In *Proceedings of Operating Systems Design and Implementation*, Carnegie Mellon University, Carnegie, USA, pp. 1–6, 2011.

[45] K. I. Shin, J. S. Park, Y. J. Lee, J. H. Park. Design and implementation of improved authentication system for android smartphone users. In *Proceedings of the 26th International Conference on Advanced Information Networking and Applications Workshops*, IEEE, Fukuoka, Japan, pp. 704–707, 2012.

[46] H. Khan, U. Hengartner. Towards application-centric implicit authentication on smartphones. In *Proceedings of the 15th Workshop on Mobile Computing Systems and Applications*, ACM, New York, USA, 2014.

[47] S. Chris, C. Nickel, C. Busch. Fingerphoto recognition with smartphone cameras. In *Proceedings of International Conference of the Biometrics Special Interest Group*, IEEE, Darmstadt, Germany, pp. 1–12, 2012.

[48] F. Schaub, M. Walch, B. Knings, M. Weber. Exploring the design space of graphical passwords on smartphones. In *Proceedings of the 9th Symposium on Usable Privacy and Security*, ACM, New York, USA, 2013.

[49] W. Z. Meng, D. S. Wong, L. F. Kwok. The effect of adaptive mechanism on behavioural biometric based mobile phone authentication. *Information Management & Computer Security*, vol. 22, no. 2, pp. 155–166, 2014.

[50] K. W. Bowyer, K. P. Hollingsworth, P. J. Flynn. A survey of iris biometrics research: 2008–2010. *Handbook of Iris Recognition*, Mark J. Burge, K. W. Bowyer, Eds., London, UK: Springer, pp. 15–54, 2013.

[51] L. Lane. International standards bodies address biometric security. *Biometric Technology Today*, vol. 2011, no. 8, pp. 2, 2011.

[52] A. Buchoux, N. L. Clarke. Deployment of keystroke analysis on a smartphone. In *Proceedings of Australian Information Security Management Conference*, Security Research Centre, School of Computer and Security Science, Edith Cowan University, Perth, Western Australia, 2008.

[53] L. Wang, R. F. Li, K. Wang, J. Chen. Feature representation for facial expression recognition based on FACS and LBP. *International Journal of Automation and Computing*, vol. 11, no. 5, pp. 459–468, 2014.

[54] I. A. Lami, T. Kuseler, H. Al-Assam, S. Jassim. LocBiometrics: Mobile phone based multifactor biometric authentication with time and location assurance. In *Proceedings of the 18th Telecommunications Forum*, IEEE, Belgrade, Serbia, pp. 151–154, 2010.

[55] J. Fenske. Biometrics in new era of mobile access control. *Biometric Technology Today*, vol. 2012, no. 9, pp. 9–11, 2012.

[56] Y. Zheng, J. C. Xia, D. K. He. Trusted user authentication scheme combining password with fingerprint for mobile devices. In *Proceedings of the International Symposium on Biometrics and Security Technologies*, IEEE, Islamabad, Pakistan, pp. 1–8, 2008.

[57] L. J. Li, X. X. Zhao, G. L. Xue. Unobservable reauthentication for smartphones. In *Proceedings of the 20th Network and Distributed System Security Symposium*, San Diego, USA, vol. 13, 2013.

[58] S. Kang, J. Kim, M. Hong. Go anywhere: User-verifiable authentication over distance-free channel for mobile devices. *Personal and Ubiquitous Computing*, vol. 17, no. 5, pp. 933–943, 2013.

[59] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, S. Ben-David. Biometric authentication on a mobile device: A study of user effort, error and task disruption. In *Proceedings of the 28th Annual Computer Security Applications Conference*, ACM, New York, USA, pp. 159–168, 2012.

Syeda Mariam Muzammal received B. Sc. degree in computer science from COMSATS Institute of Information Technology, Islamabad, Pakistan in 2012. Currently, she is a master student in computer science at COMSATS Institute of Information Techology, Islamabad, Pakistan. Her M. Sc. dissertation topic is based on Security Attacks and User′s Privacy Protection in Smartphones.

Her research interests include, security risks and threats in smartphones, ethical hacking, information security, data warehousing and expert systems.

E-mail: mariammuzammal@yahoo.com

ORCID iD: 0000-0003-2960-1814

Munam Ali Shah received the B. Sc. and M. Sc. degrees, both in computer science from University of Peshawar, Pakistan in 2001 and 2003, respectively. He received the M. Sc. degree in security technologies and applications from University of Surrey, UK in 2010, and received the Ph. D. degree from University of Bedfordshire, UK in 2013. Since July 2004, he has been an assistant professor, Department of Computer Science, COMSATS Institute of Information Technology, Islamabad, Pakistan. He is the author of more than 30 research articles published in various

conferences and journals. He also received the Best Paper Award of the International Conference on Automation and Computing in 2012.

His research interests include MAC protocol design, QoS and security issues in wireless communication systems.

E-mail: mshah@comsats.edu.pk (Corresponding author)
ORCID iD: 0000-0002-4037-3405

Si-Jing Zhang received his B. Sc. and M. Sc. degrees, both in computer science, from Jilin University China in 1982 and 1988, respectively. He received a Ph. D. degree in computer science from the University of York, UK in 1997. He joined the Network Technology Research Centre of Nanyang Technological University, Singapore, as a post-doctoral fellow in 1996, and he then returned to the UK to work as a research fellow with the Centre for Communication Systems Research of the University of Cambridge, UK in 1998. He joined the University of Derby, UK as a senior lecturer in 2000. Since October 2004, he has been working as a Senior lecturer with the University of Bedfordshire.

E-mail: sijing.zhang@beds.ac.uk

Hong-Ji Yang received the B. Sc. and M. Sc. degrees from Jilin University, China in 1982 and 1985, respectively, and received the Ph. D. degree from Durham University, UK. He served as a programme co-chair at IEEE International Conference on Software Maintenance 1999 and is serving as the programme chair at IEEE Computer Software and Application Conference 2002. He is chief editor of the *International Journal of Creative Computing*. He has published five books and well over 300 papers in software engineering, computer networking and creative computing. He is deputy director of the Centre for Creative Computing at Bath Spa University, UK.

His current research interests include software engineering and creative computing.

E-mail: h.yang@bathspa.ac.uk