Modern Authentication Techniques in Smart Phones: Security and Usability Perspective

Usman Shafique
Department of Computer Science
Bahria University
Islamabad, Pakistan

Asma Sher
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Rahim Ullah
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Hikmat Khan
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Adnan Zeb
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Rehmat Ullah
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Sabah-ud-din Waqar
Department of Computer Science
Bahria University
Islamabad, Pakistan

Uferah Shafi
Department of Computer Science
COMSATS Institute of Information Technology
Islamabad, Pakistan

Faisal Bashir
Department of Computer Science
Bahria University
Islamabad, Pakistan

Munam Ali Shah
Department of Computer Science
Bahria University
Islamabad, Pakistan

***Abstract*—A smartphone has more advanced computing ability and connectivity than basic featured phones. Presently, we are moving from the Internet society to a mobile society where more and more access to the information is required. This has resulted in a mobile security which is no longer immanent, but imperative. Smartphone authentication has received substantial attention of the research community for the past several years because there have been modern developments beyond the classical PINs and passwords making user authentication more challenging. In this paper, we critically analyze the attacks and the vulnerabilities in smartphones' authentication mechanisms. A comparative analysis of different authentication techniques along with the usage of the different authentication methods is discussed which lead the end-user towards choosing the most suitable and customizable authentication technique.**

***Keywords*—smartphone; authentication; security; attacks; knowledge-based**

I. Introduction

The rise in the usage of the smartphone over the past few years has been a technology triumph story. Latest expansions in mobile technologies have produced a new kind of device, a programmable mobile phone, the smartphone. Generally, smartphone users can program any application which is tailored for needs. Furthermore, they can share these applications in online market. Therefore, smartphone and its applications are now most prevalent keywords in mobile technology [1]. However, to provide these customized services, a smartphone needs more private information and this can cause security weaknesses. All smartphones are preferred targets of attacks. Authentication is a primary step for the safeguard of the integrity and confidentiality of an infrastructure that can only be maintained by proper identification of the end users. Authentication and authorization controls help protect unapproved access to mobile devices and the data on them. Smartphone security [2] authentication is vital for our assets that include our individual data, corporate intellectual property, classified information, financial assets, device and service availability and functionality, personal and political reputation. Authentication helps prevent data loss in the case of mobile device theft or damage. Numerous authentication techniques are proposed through which we can enhance security so that no intruder can breach the security.

A smartphone is a vital source of information. However, the availability of this information has initiated a growth in cyber-attacks. The cyber security risk to unauthorized data access is principally the same for smartphones [3][4] as it is for tablets, laptops or any other mobile device operating outside of an organization's physical offices. As more and more people use their smart cell phones to run their whole lives, hackers and others will center their efforts on getting the information they want from these devices. Regrettably, this also poses great challenges in terms of security for organizations with employees who use such devices in their day-to-day work. Data security is a chief concern not only for enterprises and small business [5], but for everyday users as well. With extensive data breaches, revealing everything from customer login credentials to credit card information to personal health records. It also stores information about your calls, your location, what you have sought on the Internet and passwords to social networks. There can be grave consequences if your phone ends up in the wrong hands [6].

Above all, you, as the owner, are considerably exposed. People in your circle of contacts can be mapped. Possibly you have sensitive contact information, business secrets, documents, minutes of meetings, customer registers or patient information accessible through your e-mails. Or even worse, a manipulated smartphone may be used as an eavesdropping [7] device or means for transporting information from, or carrying out virus attacks on your company's internal networks. Simply, being a little too forgetful plays a huge part in the growing phone theft trend. People are willing to pay big money to get their data only. Smartphones carry extremely personal information, from banking information to corporate email. Fifty percent of phone theft sufferers would be somewhat likely to extremely likely to pay $500 to regain their stolen phone's data, including all photos, videos, music, apps, and private information, while one-third of sufferers would be somewhat likely to extremely likely to pay $1,000. Even more, 68 percent of phone theft victims are ready to put themselves in some amount of danger to recover a stolen device and the valuable information on its [8]. This example evidently proves the importance of security of smartphones in the present time.

One should always be aware of the leaky applications apart from theft as unfortunately it is difficult to know what and how applications are communicating with the devices. More than half of mobile users are heedless that hackers can take control of their smartphones, according to research by Kaspersky [9]. Cybercriminals repackage malicious code in mobile applications that grants access and use these sensors in an unethical manner. Attackers can harm you in many ways for instance, he can record the conversations and send it to the third party, removal of personal and professional data [10], making phone calls forcibly, unintentional disclosure of data, financial malware attacks and thus making your phone unusable. Every week there are incidents reported about the smartphone security breaches, mobile malware and cloud services that have been hacked or compromised in some way. We all use our smartphones to keep personal and sensitive information – emails, messages, pictures, bank account details and password lists. With cloud services (e.g., iCloud, Dropbox and Google Drive) being tightly incorporated into smartphones tied with the increasing amount of digital data. Smartphones present the evil guys with a very real opportunity to steal your personal information and attack your privacy [11][12]. Data of the user is most precious in this era consequently making user authentication more challenging. The unfortunate situation is that a lot of the work done is not compared to each other highlighting the merits and demerits of the authentication schemes. In this work we will analyze vulnerabilities in smartphone authentication mechanisms, attacks related to smartphone authentication system and their pros and cons. Comparative analysis of authentication techniques discussed in this paper will lead end-users towards better decision-making for choosing the most suitable techniques.

The main objective of this paper is to analyze the modern security attacks and vulnerabilities in the authentication of smartphones. The rest of the paper is organized as follow. Section II critically review the different authentication techniques along with their limitations. In Section III, performance comparison of different smartphone authentication techniques on the basis of some parameters is performed. Section IV discusses the open issues and the paper is concluded in Section V.

II. Classification of the Smartphone Authentication Techniques

In general, the authentication process is classified into three categories, *i) something you know* (knowledge based); *ii) something you have* (possession based); and *iii) something you are* (identity based). We provide further details in the subsequent sections.

A. Knowledge-based Authentication

A knowledge-based authentication (KBA) is a security measure that identifies the users by asking them to answer specific security questions. Knowledge-based authentication has become prevalent where users are asked to answer these questions in order to gain access to personal, password-protected areas. Even though this technique is effective but still it gets difficult for people to learn the pins and passwords. In future, computers would have the ability to guess these passwords [13][14]. On the other hand, KBA can be an effective way to manage authorization for individual users, but there are also critical concerns about privacy that have been raised around the idea of using this kind of personal information for online or network security. There are two types of KBA.

- Static KBA: Static KBA [15] is also known as shared secret and is commonly used by email service providers and financial services to prove the identity of customer.
- Dynamic KBA: Dynamic KBA provides high level authentication that uses the knowledge of the user to authenticate it [15].

KBA is no longer a suitable authentication method as this technique is quite easy to break. It is easy to work out via social networking [16][17]. Social networking makes it a lot easier to work out somebody's KBA questions. For example, "what city was your father born in?". This could be worked out from one of many social networks. People can buy the Information and criminals find a lot of profit in selling the data in black market [18]. Different security firms and organizations are actively seeking to improve their security with a layered approach in line with the recommendations of the leading security experts and analysts.

B. Possession Based Authentication

This technique is also known as 'token-based authentication'. Its use is to basically check the user's validity. The token is generated by using the username and password of the users. The user can then use that token at other places which will grant them access to those places without having them put their usernames and passwords. This token will however let them access till a specific time period. In short, a token is provided to the users based on their login credentials. This token lets them access their protected resources till a limited time, without using their credentials repeatedly. The token mostly consists of a string that is of 32 characters. After the user enters his login credentials, the generated token is associated with the database in some way. The user can utilize the token to access other contents of a similar application. This is the reason why the received token has to be saved once it's retrieved. Tokens [19] are stateless and scalable as they hold the data for that user themselves. This technique provides security in a way that token also expires after a set amount of time, so a user will be required to login once more. This helps us stay safe. There is also the idea of token revocation that lets us to nullify a specific token [20][21] and even a group of tokens based on the same authorization allowance.

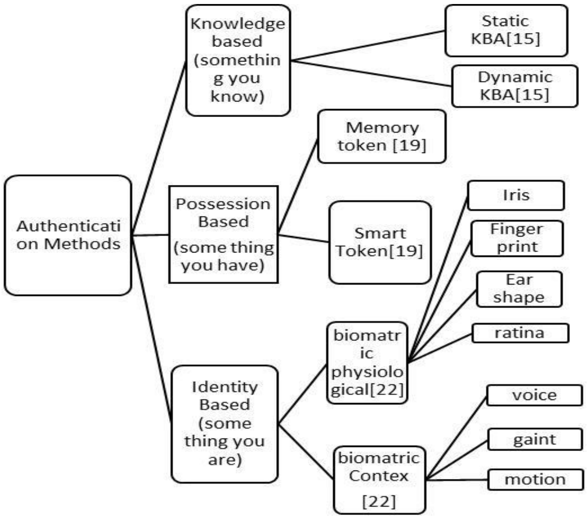

Fig. 1. Classification of authentication methods

C. Biometric Based Authentication

The design of a biometric system includes a special hardware that is connected with a processing hardware through a sensor. The separation of the parts is prone to external attacks. However, the use of cryptography can secure the system. This is done by splitting up the private cryptography key of all systems, generating limited vectors from the system to be used as keys and then calculating a hash function for all those keys. The same process is done for each trait and the hash functions are stored in a database that is kept unlimited [22]. These hash values are basically used for identification purposes. The user would enter a biometric attribute which would consequently be converted into the particular hash value and the results will be checked accordingly. This method is carried out for all parts of the cryptographic key corresponding to different traits and the resulting private key is deleted after use. [23] There is a possibility to use all the traits at once but using them separately decreases the chance of misuse and fraudulent attacks. Biometric based authentication techniques, such as fingerprints, iris scan, or facial recognition, are not yet widely adopted as this approach can be expensive, and the identification process can be slow and often unreliable i.e. it is not reliable since it is time consuming. Figure 1 shows the classification of different authentication techniques.

III. Modern Authentication Techniques

In this section, we give an overview of different authentication techniques which are currently being used in smartphones.

A. Slide Lock

In this authentication scheme the primary objective is to prevent an unauthorized person from using any false key [24]. He can easily breach security due to Boolean password key space true or false.

B. Number Lock, Pin code and Password

4-digit based password scheme provides much security when compared with the slide lock but still it has weak security because less password key space brute force attack is possible 0 to 9999 are password space [24]. This is the simplest method and is easy to break by brute force attack. Here if the user selects a simple code it will be easy to remember and easy to enter, but it will be difficult to break also. According to survey, 56% people enter wrong password because their length is limited [25]. PINs are open to accept surfing and systematic trial and error attacks. Number Lock or Pin codes must be encoded otherwise in the case of a mobile database application i.e., a distributed database there are security trials due to the distributed nature of the application and the hardware limitations of mobile devices. The major issues in multilevel security are authentication, data confidentiality, identification and accessibility [26]. This technique is user friendly and easy, less time consuming and has large address space. Nevertheless, it can be affected by Brute Force Attack, stored passwords can be accessed in some way, password gets revealed while logging in a public place and there is always a chance of conflict with other passwords. This system may also go through impersonation in which an unauthorized person can steal confidential data using password and ID.

C. Graphical Based Password

Due to some weaknesses in text based password scheme and also it is difficult for human to memorize long passwords, [27] Blonder *el at* proposed graphical password based technique. This technique is further classified into two types: *i) Recall based technique* and *ii) Recognition based technique*. In a recall based technique, a user is required to draw image which he has created in registration phase. Draw-a-secret scheme, Signature scheme and Pass-points scheme are examples of this scheme. In a recognition based technique, [24], users are required to identify image and recognized image which he has selected in registration phase. Bhanushali *et al.* compare different graphical password algorithm [28] security and most appropriate algorithm among them is "pass-point" which resistance against many attacks. M. Alia *el at* [29] proposed another graphical password scheme that based on different shapes that resist against many attack but still time consuming process. Authentication process based on color code user has to arrange true color sequence which he has performed in registration phase a proposed by [30] S.Bandare *el at* are resist to many different attack but still much processing are involved in that scheme. Figure 2 represents the Graphical authentication methods.

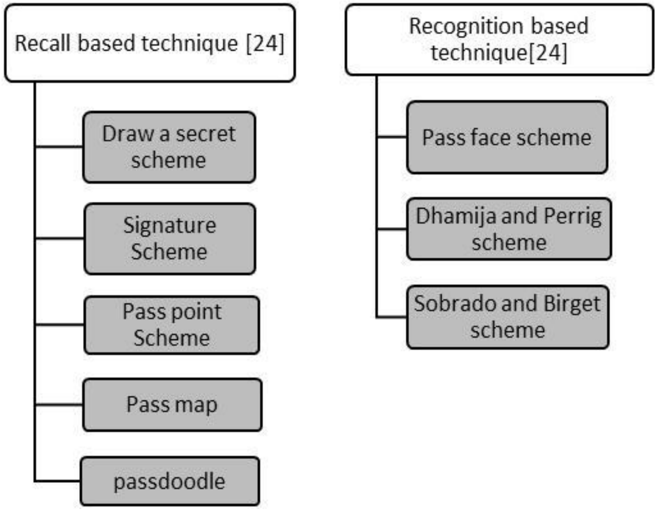
Recall based technique [24]
Draw a secret scheme
Signature Scheme
Pass point Scheme
Pass map
passdoodle
Recognition based technique[24]
Pass face scheme
Dhamija and Perrig scheme
Sobrado and Birget scheme

Fig. 2. Classification of Graphical Password Scheme

D. Fingerprint Recognition

In fingerprint recognition, the complete process consists of six different steps. The first step is to get a high quality image of the fingerprint input so that it is easily identified by the automated system. The next step is to improve the image quality to remove any grooves and ridges that are affecting it. [31]. This is done by obtaining histogram images and then applying filter over it. Image is preprocessed then using the technique of thresholding by RAT scheme (Regional Average Thresholding) and thinning (by Emyroglu). The next step includes fingerprint classification in five classes which is a little for both the machine and human because of the complication of fingerprints. The details are extracted afterwards using the Emyroglu extractor. The last step is verification where two minutiae sets are compared. Ratha method [32] is used for the comparison purposes. The intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords. It is more secure, faster, reliable, simple and user-friendly but it is expensive as it requires large size devices and use is difficult. On the contrary, there is always a probability of Brute Attack involving a set of fraudulent fingerprint minutiae. One way to enhance security is to use data-hiding techniques to embed additional information directly in compressed fingerprint images. For instance, if the embedding algorithm remains unknown, the service provider can look for the appropriate standard watermark to check that a submitted image was indeed generated by a trusted machine (or sensor). Nonetheless, Replay attacks have been addressed using data-hiding techniques [33] to secretly embed a telltale mark directly in the compressed fingerprint image.

E. Speaker Recognition

The speaker recognition comprises of four parts. The first part is the recording of the signals that is done by the use of a sound hardware. Then the input signals are preprocessed by pre-emphasis, framing, windowing and clipping of the non-speech frames, i.e. selecting of the speech frames. Then comes the method of feature extraction where the frames extracted from input signals are further processed to recognize some particular features. The last step is recognition that results in either complete acceptance or complete denial. It mainly depends on the set of features that were chosen [34]. However, the feature set that is chosen may not be correct so some other tools have to be used to recognize the speaker. This way is reliable as no two people have same voice [35] Positive points include non-intrusive nature, high social acceptability, verification time about 5 seconds and nominal. On the other hand, one can record the voice for unauthorized use. Voice quality can be affected by disease. This system is not very user friendly as there is always a difference of pronunciation and accents. The system can be attacked by using human and algorithmic attacks. For the initial scenario (human), a subject is requested to say the pass-phrases of the target users for multiple sequences. For the first round, the frauds say the pass-phrases without hearing the target voice. In the second round, they are requested to copy the pass-phrases of the target users by hearing the voice of the target users. In this round, it is confirmed that the subjects are well-motivated by providing a motivation incentive for the best copier. For the next scenario (algorithmic), it will contain the usage of voice recordings from the target users to make manufactured pass-phrases. The synthesized sound will be made from modern technologies; we use HMM-based speech synthesizer. The collection of the voice data is sensibly designed [36], so the voice would not overlap with the pass-phrases of the target users. In the final scenario (algorithmic), we re-generate users' pass-phrases built on the template information. Then, these pass-phrases will be used to attack the systems. Many biometrics are susceptible to attack [37] because some information is leaked from the biometric template.

F. Iris Recognition

This technique uses the unique patterns of human eye as an authentication measure. The pupil is used to recognize the user's identity and the smartphone is accessed only when the pupil matches with the user's pupil. Special hardware has to be installed in mobile phones for this purpose. This reduces the risk of theft and fraudulent attacks to a large extent. All smartphone companies [38] are trying to install this feature in their devices in the future. Among other biometric systems, this provides higher security. Using IRIS recognition system, the overall accuracy is to be 99.92% [39]. Merits of this system include stability, relatively compact and efficiency. Although this technique authenticates the person but it is expensive, requires a lot of memory for image storage and not very user-friendly. Fake and reconstructed iris patterns can be presented to iris sensor input for carrying out an attack on the system.

G. Face Recognition

Face recognition technique is considered the best among all other biometric authentication techniques. This is because all other techniques require some kind of contact whereas face recognition does not involve any kind of contact with the user. The user’s face can be recognized from a large distance. This technique also helps in future crime investigations [40] because the stored information can be use further to identify a particular person. This system is defeated by natural changes in environment such as lighting and posing [41] [42]. A facial recognition system is an application system in which digital image is used for automatically identifying a person or authenticates users. Initially system stores a part of face (area of interest) in database and then the image taken by the camera is compared with the image stored in database [37]. This technology is simple, easy to implement and use and not so expensive. Whereas, 2D images can be affected by light, person’s age, hair and glasses as facial system use camera so must have a camera for acquiring images. Anyone can break into this system if we bring the image of the valid person through another device and system would be easily logged in.3D masks are used to spoof 2D face recognition systems.

H. Palm Vein Authentication System

Bio-metric validation technology identifies individuals by their one of a kind natural biological data. Since veins are inside to the human body, its data is difficult to imitate. Compared with a finger or the back of a hand, a palm has a more extensive and more complex vascular example and thus contains an abundance of recognizing elements for individual's distinguishing proof. Palm vein validation utilizes an infrared beam to enter the client's hand as it is held over the sensor; the veins inside of the palm of the client are returned as gray lines. As every Bio-metrics technology has its benefits and shortcomings, it is hard to make direct comparisons, but since vein validation depends on natural data within the body, it is more successful than the others at lessening the probability of falsification. Likewise, vein design acknowledgment needs only an output of the palm, therefore making it the least demanding and most characteristic to use amongst the different biometric advances [43]. In addition, to affirm the precision of individual validation to a much greater degree, vein acknowledgment can be joined with face acknowledgment frameworks to bolster "multimodal confirmation" that ensures exactness through different layers of safety. Notwithstanding better security, vein confirmation utilized as a part of mix with face acknowledgment frameworks would likewise keep a record of facial data to be utilized as a proof [44]. The recognition rate is very good using palm vein [45]. Experiments show that this approach is feasible and effective [46]. False acceptance rate is 0.0008% and false reject rate is 0.01% [47]. It is safer, faster, reliable and improving performance. It is complicated at first, expensive, cannot be used in simple devices and not very much user-friendly. A principle advantage of biometric authentication is that biometric information is based on physical attributes that stay steady all through one's lifetime and are hard to fake or change. Fingerprints, palm vein, and iris outputs can yield absolutely special information sets when finished properly. It is difficult to characterize which technique for biometric information assembling and reading does the "finest" job of affirming secure authentication. Each of the distinctive methods has in-built advantages and disadvantages. Biometrics-based validation has numerous usability advantages over conventional frameworks [48], for example, passwords. Exactly, clients can never lose their biometrics, and the biometric signal is hard to take or manufacture. Yet, any framework, including a biometric framework, is helpless when assaulted by determined hackers. When an arrangement of biometric information has been compromised, it is compromised forever.

I. Brain Wave Based Authentication

The model is partitioned into two primary parts separated from EEG headset. A front-end part set on a cell phone in charge of client communication and a back-end part set on a remote server in charge of preparing EEG information and taking care of the validation calculations [49]. Short EEG recordings can be changed to speak to one of a kind bio-metric identifiers, including both: behavioral and physiological qualities. Sensor condition and adjustments of the EEG headset are essential for effective system usage [50]. On the off chance that stress signs are available in the measured brainwaves it will bring about a refusal of access, hence, making it an unbreakable framework. The benefits over different frameworks are numerous. With a standard password somebody can lookout or "shoulder-surf" what others write, yet none can watch thoughts. Cards and keys can be lost, however the brain dependably there. Handicaps can preclude individuals from frameworks like fingerprint-or retina scanners, yet the mind still works [51].

J. Recognition of 2D and 3D Gestures

2D gestures are also being used as an authentication technique. It involves two kind of approaches. One is the use of hand-coded algorithms whereas the other approach relates to the features. The features are first used to take the input of coordinates and then an algorithm is applied to recognize that gesture. As far as 3D gestures are concerned, they make use of the motion dynamics to monitor the gestures [52]. This system is configurable, trainable and resilient to false users [53]. Despite this system being highly secure, it is somehow affected by Shoulder surfing attacks and successful efforts are being made to overcome this threat.

K. The Use of Pseudo Pressure in Authentication

A new technique has been introduced for user authentication; it is the use of pseudo pressure. It consists of pseudo touch pressures that are used as an increased security measure for the typical digit locks security technique. This technique allows the user to select the amount of pressure he would exert on the selected security keys [54]. The database system then records the chosen key of user along with the amount of pressure that is applied on that particular key. This saved data is used every time the user has to login to his smartphone. The device is unlocked only when both the stored and recently entered key and pressure matches [55]. It is slower and more error-prone, but performs considerably better in short term. Also, most users felt safer using it and wanted to use it on their smartphones. It is affected by smudge attacks but comparatively more resistant to them in comparison to digital-lock technique. A study confirmed that it does increase security by making it fairly more resilient to smudge attacks and less susceptible to situations where attackers are already in possession of users' passwords [56]. Thus making it a better technology than digital-lock technique.

L. Keystroke-dynamics based User Authentication

It is a unique method which lets the system to authenticate the users based on their keystrokes and the time duration is noted. The time duration has a specific name; digraph. When studied further, researchers made use of additional parameters by making combinations of the keystroke. A recent study reported that keystroke authentication had been proved really helpful in recognizing imposters and fraudulent attacks on users' accounts [57]. This biometric system does not need any added sensor. As it is usual for everyone to type a password for authentication purposes making user's acceptability high. This kind of biometric system respects the secrecy of users. Indeed, if the biometric pattern of an individual has been taken, the user just has to change its password. Keyboard Dynamics, being one of the inexpensive methods of biometric, has a pronounced scope. Spyware is a software that registers information about users, usually without their knowledge. Spyware is perhaps the finest and easiest way to crash keystroke dynamic-based authentication systems. This system is can be affected to Brute force attacks and dictionary attacks but still less vulnerable than text based passwords. Reports on real cases of cracking keystroke dynamics authentication system [58] are not existent.

M. Location based Authentication

Many of the smart phone uses location based authentication to provide security solutions to the users. Many smartphones are equipped with GPS to detect the user's locations. Some of these location tracking systems are Google Maps, Yelp, Foursquare etc. Much of the work is still being done in this area by improving the techniques. For this reason, they are using a massive amount of databases and access towers [59]. This has supported the measurement of user's location within some meters. These locations based techniques involve special devices and a specific setup that is essential for defining the locations. This is the purpose why these systems are hard to implement. The special requirements for their application are difficult to implement. [60]. The threats to this kind of system include: *Threats by close oppositions that use the Internet for exploring the answers* and *Threats by strangers that also use the Internet for research to perform educated estimates* [61]. Nevertheless, the accuracy values as well as the number of false positives and false negatives are promising eventually making it a better technology.

N. Context based Authentication

Traditional authentication systems are vulnerable for highly dynamic environments. Often uses traditional authentication systems in mobile devices. These are vulnerable for highly dynamic environments, therefore in such environments need of new approaches to be implemented. These new approaches must be context aware of environment and customizable that a user wants to have over his systems [62]. Here user can be authenticated by using data captured by sensors at of the mobile device and the behavior of the user. Here a unique profile will be maintained for the user. Mobile device will identify the user by the behavior e.g. for how long the user uses a specific application, how the user uses a mobile, how the user press buttons and screen etc. here the problems can be that other people can adopt the behavior of the user [63]. Context based authentication offers convenient and strong authentication. System first go through a training session and gain some information about the user and after that when the user himself picks mobile, device first check whether valid user or not. Here users do not enter any things. User just starts his work and mobile device tests the user in that short instant of time [64]. Highly positive event is when correct explicit authentication occurs and highly negative event is when a failed explicit authentication occurs. The result shows that a False Accept Rate (FAR) of 4.46% and False Reject Rate (FRR) of 0.13% achieved. The low values indicate that excellent security is access without disturbing the mobile user. It is very easy to use [65], no need of extra time to enter something, more flexible than other. But expensive, need complex sensors for manufacturing cannot be used in simple devices. Context-based authentication is a powerful, layered approach that limits the ability of attackers to move laterally within your organization and use any credentials they compromise or create to steal valuable intellectual property, financial data, or other sensitive information.

O. Radio Frequency Identification (RFID) based Authentication

The mobile devices have a RFID device and will recognize the user by his tag using radio frequency technology. But here the problem is that the tag of someone can be copied by others and then can use his mobile device. For the solution active tags are required which are difficult to create and are expensive also [66] [67] [68]. In RFID data is transfer through wireless electromagnetic field; here tags are used for the automatic identification. Information stored in tags by electronically. Electromagnetic induction is produced by the tags near the reader. Radio waves are used in some type of tags in the form of energy. Some type of tags uses a local power source (battery) and may work at hundreds of meters away from the reader [68]. The active tags are very useful but are very much expensive and passive tags are very simple and are cheap but the problem is that simple chip can be copied or steal by malicious user. It has many advantages such as RFID tags can be read from greater distance.

It is not necessary to position all the tags in line from the scanner. It can be read at a faster rate than barcodes. Up to 300ft the information can be read from tags. RFID tags are used as read and write devices. RFID tags are reusable at other time and they are protected by a plastic cover [69]. But more expensive, harder to understand, less reliable. Tags are often larger and heavy, user feel uncomfortable to have it all the times, possibility of unauthorized reading. 37% people did not use the passwords on the account of the fact that they were time taking as they had to enter it every time they wanted to use their device and found it difficult to remember the passwords. Rest of the 63% majority [70] used authentication techniques out of which 56% used pattern authentication scheme considering it quicker and easier to memorize for the sake of authentication and typing passwords was becoming cumbersome for the people [70]. More than 30% of the people told that they often mistype their passwords because of small keys and ultimately remove password after getting frustrated.

The situation gets even worse when the people have to use strong and complex passwords [70] forcing them to choose easy and weak passwords or no passwords at all. More than 60% people conveyed that they were to unlock their devices 15 times on an ordinary daily. Typing passwords every time was tiresome for them and a majority of 90% wants a quicker and easier solution for authentication schemes used in their smartphones Figure 3 presents the statistics of authentication method used.

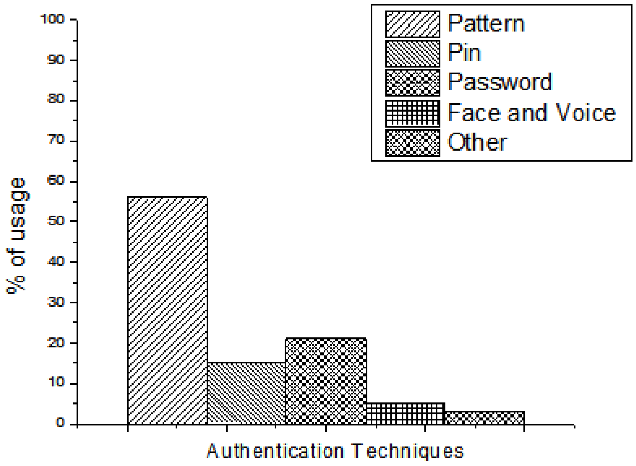

Fig. 3. Usage of different authentication methods

TABLE I. LEVEL OF SECURITY FOR DIFFERENT SMARTPHONE AUTHENTICATION TECHNIQUES

Technique Name	**Brute Force**	**Shoulder Surfing**	**Smudge Attack**	**Dictionary Attack**	**Spyware**
Side Lock [24]	Yes	Yes	Yes	Yes	Not Defined
Pin/password [24][25]	Yes	Yes	Yes	Yes	Yes
Graphical based Password [28][29][30]	Yes	Yes	Yes	Yes	Not defined
Finger Print [32][33]	Yes	No	No	Yes	Yes
Speaker recognition [34][35]	Yes	No	No	Yes	Not defined
Iris Recognition [38][39]	Yes	No	No	Yes	Not defined
Face Recognition [37]	Yes	No	No	No	Not defined
Context Based Authentication System [65][65]	No	No	Yes	No	Not defined
Palm Vein Authentication System [43][43]	No	No	No	No	No
Brain Wave Based Authentication [51]	No	No	No	No	No
Location-based Authentication [59][60][61]	No	No	No	No	Yes
Recognition of 2D and 3D gestures [53]	No	Yes	Not defined	No	Not defined
Pseudo Pressure in Authenticating [55]	Yes	No	Yes	No	Not defined
Keystroke-dynamics based [57][58]	Yes	Not addressed	Not defined	Yes	Yes
RFID[68]	No	No	No	No	Yes

IV. DISCUSSION AND OPEN ISSUES

After analyzing different smartphone authentication techniques that are discussed in previous sections, it could be observed that every authentication mechanism has its own merits and demerits and their cannot be a perfect choice. In Table 1, we have performed a comparative analysis of each technique while in Table 2, the security level of each technique is provided. Based on these analyses, the users have to see his/her own circumstances and ease of use in order to select an authentication technique as their preferred choice.

TABLE II. COMPARATIVE ANALYSIS OF DIFFERENT AUTHENTICATION TECHNIQUES FOR SMARTPHONES

Technique Name	User friendly	Computational cost	Security	Reliable	Fast Authentication	Resource requirement	Merits & Demerits
Slide Lock [24]	Yes	No	Weak	No	Yes	Uses Boolean Logic	Easy, less time taking, User friendly but easy breakable
Pin/password [26]	Yes	No	Weak	No	Yes	String comparison only	Breakable, Conflict in passwords
Graphical based passwords [26][28-30]	Yes	Yes	Intermediate	Intermediate	Intermediate	Database requirement	Better to memorize graphical passwords, reliable and accurate. More difficult to break than Text based passwords. Not widely used, storage requirement
Finger Print [31-33]	Yes	Yes	Intermediate	Yes	Yes	Database requirement	Secure, Reliable, Fast, Needs extra expensive device, large sized.
Speaker recognition [34][35]	No	No	weak	Yes	No	Database requirement	Reliable, less expensive, Sound can be recorded, Includes the effect of disease.
Iris Recognition [38][39]	Yes	Yes	Intermediate	Yes	Yes	Memory requirement	Accurate, Stable, Affected by diseases, Expensive
Face Recognition [37]	Yes	Yes	Intermediate	Yes	No	Database and Memory requirement	Simple, Easy implementation, less expensive, Effect of hair, light and glass
Palm Vein Authentication [43-46]	Yes	Yes	Strong	Yes	Yes	Memory requirement	Good Performance, cannot be used in simple
Brain Wave Based Authentication [49][51]	No	Yes	Strong	Yes	Yes	Extra sensor and memory requirement	Strong authentication, not breakable, complex and connate be used in ordinary mobiles.
Context Based Authentication system [62]	No	Yes	Strong	Yes	Yes	Extra senor and memory requirement	Easy, fast, Expensive, complex sensor
Location Based Authentication	Yes	Yes	Weak	No	Yes	Extra senor required	Low accuracy due to incorrect positioning, User friendly, Expensive, Hard to Implement, Breakable.
Recognition of 2D and 3D Gestures [52]	No	Yes	Strong	Yes	Yes	Memory requirement	Configurable, trainable and Resilient to false users. Breakable somehow by Shoulder surfing, Surfing attacks, Complex.
Pseudo pressure in Authentication [54-56]	No	No	Intermediate	Yes	No	Database requirement	Performs considerably well in Short term, more resilient than digital lock technology, slow, error prone.
Keystroke dynamics based [57][58]	Yes	No.	Weak	Yes	Yes	Memory requirement	Requires no added sensors, Inexpensive, respects the secrecy of users, high user Acceptability Breakable and weak in terms of Security.
RFID [66-69]	No	No	Strong	Less	Yes	Extra senor and memory requirement	Faster, user friendly, Tag can be reused. Complex, Less reliable, Expensive

V. CONCLUSIONS

The value of data is steadily expanding; perhaps considerably more than the actual money and threats to mobile phones are pervasive. Everyday mobile users and enterprises are confronting some or other sort of attacks like malware, loss and theft, exploitation, communication interception, and many more. With effective utilization of security systems as said above, organizations and people can cost-effectively prepare for present and rising threats, while holding optimal efficiency and adaptability in their use of smartphones. In this paper, we compared the usability and security level of different authentication methods for smartphones. There is a trade-off among these frameworks; if a system is much secure then it will be expensive and less user friendly and the other way around. Every technique discussed above is somehow breakable and requires improvement in some way or the other. In this paper, by reviewing the pros and cons of various available authentication schemes, we provided a substantial overview on the authentication solutions for the mobile devices. In present, there are numerous researches on cell phone security, yet there is a lack of effort to analyze all security threats of mobile devices.

References

[1] Guo, C.,Wang, H.J., Zhu, W.: Smart-Phone Attacks and Defenses. In: HotNets III (November 2004)

[2] N. Leavitt, "Malicious Code Moves to Mobile Devices," IEEE Computer, vol. 33, no. 12, 2000".

[3] D. Dagon et al., "Mobile Phones as Computing Devices: The Viruses are Coming!" IEEE Pervasive Computing, vol. 3, no.4,2004.

[4] Smartphone: Information security risks, opportunities and recommendations for users, ENISA Report (December 2010)

[5] Li, Qing, and Greg Clark. "Mobile security: A look ahead." Security & Privacy, IEEE 11.1 (2013): 78-81.

[6] La Polla Mariantonietta Fabio Martinelli and Daniele Sgandurra "A survey on security for mobile devices" communications surveys & tutorials, IEEE 15.1 (2013):446-471

[7] De Luca, Alexander, et al. "Back-of-device authentication on smartphones. "Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 2013.

[8] Dörflinger, Tim, et al. ""My smartphone is a safe!" The user's point of view regarding novel authentication methods and gradual security levels on smartphones." Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on. IEEE, 2010.

[9] Bojinov, Hristo, and Dan Boneh. "Mobile token-based authentication on a budget." Proceedings of the 12th Workshop on Mobile Computing Systems and Applications. ACM, 2011.

[10] Zhou, Yajin, and Xuxian Jiang. "Dissecting android malware: Characterization and evolution." Security and Privacy (SP), 2012 IEEE Symposium on. IEEE, 2012.

[11] Enck, William, Machigar Ongtang, and Patrick McDaniel. "On lightweight mobile phone application certification." Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009.

[12] Theoharidou, Marianthi, Alexios Mylonas, and Dimitris Gritzalis. "A risk assessment method for smartphones." Information Security and Privacy Research. Springer Berlin Heidelberg, 2012. 443-456.

[13] A. K. Jain, A. Ross, S. Prebake, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20, January 2004.

[14] K. Revett, PhD, Behavioral Biometric A Remote Access Approach, Wiley, UK,

[15] S. A. Manjunath D., Nagesh A.S., Sathyajeeth M.P., NaveeKumar J.R., "A Survey on Knowledge-Based Authentication," J. Emerg. Technol. Innov. Res., vol. 2, no. 4, pp. 1194–1201, 2015.

[16] Smartphone: Information security risks, opportunities and recommendations for users, ENISA Report (December 2010)

[17] M. Balduzzi, C. Platzer, T. Holz, E. Kirda, D. Balzarotti, and C. Kruegel. Abusing social networks for automated user profiling. In Recent Advances in Intrusion Detection: 13th International Symposium, RAID 2010, Ottawa, Ontario, Canada, September 15-17, 2010, Proceedings, volume 6307, page 422. Springer-Verlag New York Inc, 2010.

[18] M. Egele, C. Kruegel, E. Kirda, and G. Vigna. Pios: Detecting privacy leaks in ios applications. In Network and Distributed System Security Symposium (NDSS), 2011

[19] A. K. Jain, P. Flynn, A. ROSS, Handbook of Biometrics, Springer, USA, 2008.

[20] XMPP Foundation. XMPP Standard, 2011. [Online; retrieved Jun 21st, 2011], http://xmpp.org/l.

[21] H.Falaki,R.Mahajan,S.Kandula,D.Lymberopoulos,R.Govindan,n dD.Estrin. Diversity in smartphone usage. In MobiSys, 2010.

[22] Anneke Kosse, "Do newspaper articles on card fraud affect debit card usage?," Journal of Banking & Finance, (2013)

[23] Ihsan A. Lami, Torben Kuseler, Hisham Al-Assam, and Sabah Jassim, "LocBiometrics: Mobile phone based multifactor biometric authentication with time and location assurance," Proc. 18th Telecommunications Forum IEEE TELFOR, (2010)

[24] K. Il Shin, J. S. Park, J. Y. Lee, and J. H. Park, "Design and Implementation of Improved Authentication System for Android Smartphone Users," pp. 2–5, 2012.

[25] DiCarlo, James J., Davide Zoccolan, and Nicole C. Rust. "How does the brain solve visual object recognition?." Neuron 73.3 (2012): 415-434.

[26] S.Schroeder. Smartphones Are Selling Like Crazy. http://mashable.com/2010/ 02/05/smartphones-sales/.

[27] M. R. Albayati and A. H. Lashkari, "A New Graphical Password Based on Decoy Image Portions (GP-DIP)," vol. I, pp. 295–298, 2014.

[28] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of Graphical Password Authentication Techniques," vol. 116, no. 1, pp. 11–14, 2015.

[29] M. Alia, A. Hnaif, H. Al-Anie, and A. Tamimi, "Graphical Password Based On Standard Shapes," Sci. Ser. Data Rep., vol. 4, no. 2, pp. 71–79, 2012.

[30] S. R. Bandre, "Design and Implementation of Smartphone Authentication System based on Color-code," vol. 00, no. c, 2015.

[31] D Denning and P MacDoran, "Location-Based Authentication: Grounding Cyperspace for Better Security," Computer Fraud and Security Bulletin, (1996)

[32] Torben Kuseler and Ihsan Alshahib Lami, "Using Geographical Location as an Authentication Factor to enhance mCommerce Applications on Smartphones," International Journal of Computer Science and Security (IJCSS) 6(4), 277-287 (2012) [7] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," Proc. of the 10th workshop on Mobile Computing Systems and Applications, New York, NY, USA, 3:1--3:6 (2009)

[33] Wimberly, Hugh, and Lorie M. Liebrock. "Using fingerprint authentication to reduce system security: An empirical study." Security and Privacy (SP), 2011 IEEE Symposium on. IEEE, 2011.

[34] J.-P. Aumasson and D. Khovratovich, First analysis of Keccak, Available online, 2009. [12] D. J. Bernstein, Second preimages for 6 rounds of keccak, 2010.

[35] Rabiner, Lawrence R. "A tutorial on hidden Markov models and selected applications in speech recognition." Proceedings of the IEEE 77.2 (2011): 257-286.

[36] Ververidis, Dimitrios, and Constantine Kotropoulos. "Emotional speech recognition: Resources, features, and methods." Speech communication 48.9 (2013): 1162-1181.

[37] Swaminathan, A., N. Kumar, and M. Ramesh Kumar. "A Review of Numerous Facial Recognition Techniques in Image Processing." (2014).

[38] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, RADIOGATUN, a belt-and-mill hash function, Second Cryptographic Hash Workshop, Santa Barbara.

[39] Venugopalan, S. and Savvides, M., "How to generate spoofed irises from an iris code template," IEEE Trans. on Information Fonrensics and Security 6, 385–394 (2011).

[40] J. Galbally, C. McCool, J. Fierrez, S. Marcel, On the vulnerability of face verification systems to hill- climbing attacks, Pattern Recognition 43 (2010) 1027–1038.

[41] Jenkins, Rob, and A. M. Burton. "100% accuracy in automatic face recognition." Science 319.5862 (2008): 435-435.

[42] Zhao, Wenyi, et al. "Face recognition: A literature survey." ACM computing surveys (CSUR) 35.4 (2003): 399-458.

[43] Masaki Watanabe Toshio Endoh Morito Shiohara and Shigeru sasaki ," Palm vein authentication technology and its applications",The Biometric Consortium Conference, September 19-21,2011,USA

[44] Muhammad Imran Razzak, Rubiyah Yusof and Marzuki Khalid,"Multimodal face and finger veins biometric authentication",Scientific Research and Essays Vol. 5(17), pp. 2529-2534, ISSN 1992-2248 ©2010 Academic Journals.4 September, 2010.

[45] Zhang, Yi-Bo, et al. "Palm vein extraction and matching for personal authentication." Advances in Visual Information Systems. Springer Berlin Heidelberg, 2013. 154-164.

[46] Han, Wei-Yu, and Jen-Chun Lee. "Palm vein recognition using adaptive Gabor filter." Expert Systems with Applications 39.18 (2012): 13225-

13234.

[47] Watanabe, Masaki, et al. "Palm vein authentication technology and its applications." Proceedings of the biometric consortium conference. 2011.

[48] Bhudev Sharma, “Palm Vein Technology”, Technical Report, Electronics Engineering Department, National Institute of Technology, India, 2010

[49] C. Ashby, A. Bhatia, F. Tenore, and J. Vogelstein, “Low-cost electroencephalogram (EEG) based authentication,” 2011 5th International IEEE/EMBS Conference on Neural Engineering (NER), IEEE, 2011, pp. 442–445.

[50] J. Rønager, Interview and Meeting about EEG and authentication., Aalborg University Copenhagen: 2012

[51] Y .Renard F. Lotte, G Gibert, M. Congedo, E. Maby, V. Delannoy, O. Bertrand, and A. Lecuyer, “Open VibE: An Open Source Software Platform to design , Test and Use Brain-Computer Interfaces in Real and Virtual Environments,” Presence: Teleoperators and Virtual Environmrnts, vol. 19,Feb. 2010,pp.35-53

[52] Aumasson and W. Meier, Zero-sum distinguishers for reduced Keccak-f and for the core functions of Lu_a and Hamsi, Available online, 2009.

[53] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon. Biometric-rich gestures: a novel approach to authentication on multi-touch devices. In Proc. of CHI ’12.]

[54] Shacham, H.: The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86). In: Proceedings of the 14th ACM conference on Computer and Communications Security (CCS 2008), pp. 552–561. ACM, New York (2007)

[55] Buchanan, E., Roemer, R., Shacham, H., Savage, S.: When Good Instructions Go Bad: Generalizing Return-oriented Programming to RISC. In: Proceedings of the 15th ACM conference on Computer and Communications Security (CCS 2008), pp. 27–38. ACM, New York (2008)

[56] Jakobsson, M. and Akavipat, R. Rethinking passwords to adapt to constrained keyboards. MoST Workshop '12, IEEE (2012).]

[57] Garg, Urvashi, and Yogesh Kumar Meena. "User authentication using keystroke recognition." Proceedings of International Conference on Advances in Computing. Springer India, 2012.

[58] Multiplying Mobile: How Multicultural Consumers Are Leading Smartphone Adoption. Nielsen. Mar. 04, 2014. http://shar.es/N0VNj

[59] S. Holtmanns, V. Niemi, P. Ginzboorg, P. Laitinen, N. Asokan, Cellular Authentication For Mobile And Internet Services, Wiley, UK, 2012.

[60] Sailer, R., Zhang, X., Jaeger, T., van Doorn, L.: Design and Implementation of a TCG-based Integrity Measurement Architecture. In: SSYM 2011: Proceedings of the 13th conference on USENIX Security Symposium, Berkeley, CA, USA. USENIX Association (2011)

[61] E. Stobert and R. Biddle. The password life cycle: User behavior in managing passwords. In Proc. SOUPS 2014, pages 243– 255. USENIX, 2014

[62] Lima, Joao Carlos D., et al. "A Context-Aware Recommendation System to Behavioral Based Authentication in Mobile and Pervasive Environments."Embedded and Ubiquitous Computing (EUC), 2011 IFIP 9th International Conference on. IEEE, 2011.

[63] Jakobsson, Markus, et al. "Implicit authentication for mobile devices."Proceedings of the 4th USENIX conference on Hot topics in security. USENIX Association, 2012. Dandachi, Ghina, Bachar El Hassan, and Anas El Husseini. "A novel identification/verification model using smartphone's sensors and user behavior."Advances in Biomedical Engineering (ICABME), 2013 2nd International Conference on. IEEE, 2013.

[64] Feng, Tao, et al. "Continuous mobile authentication using touchscreen gestures." Homeland Security (HST), 2012 IEEE Conference on Technologies for. IEEE, 2012.

[65] Kale, Rahul, et al. "Review paper on two factor authentication using mobile phone (Android)." Journal of Computer Engineering and Informatics 1.3 (2013): 99-102.

[66] Kim, Dong Seong, Taek-Hyun Shin, and Jong Sou Park. "A Security Framework in RFID Multi-domain System."

[67] Ko, Chien-Ho. "Applying RFID Technology in Building Maintenance."

[68] Malika Verma, Monica Sood, Smarter Method for User Authentication in Mobile System 1Malika Verma, 2Monica Sood, International Journal of Advanced Research in Computer Science and Software Engineering 2015.