Next Level User Authentication in Android

[1]Pulkit Tandon, [2]Geogen George
[1]M.Tech Scholar, [2]Assistant Professor
[1]I.T Dept., SRM University, Chennai, Tamil Nadu, India
[2]I.T Dept., SRM University, Chennai, Tamil Nadu, India
[1]pulkit.tandon0505@gmail.com, [2]geogen007@gmail.com

Abstract: **Device security are the major challenges faced by the smartphone developers in the recent era to secure the E-Data from security breaches. The finest possible alternative present due to limited range of current methods is to concatenate existing data security method with novel procedures which should be quick-to-implement and at the same time should be highly secure. The paper aims to strengthen the data security on the device by creating a custom user for the device other than the device administrator. The administrator is authenticated through speech recognition and pattern recognition methods whereas the custom user is verified using PIBRAS.**

Keywords: **Shoulder Surfing, Brute Force Attack, Custom User, Speech Identification, MFCC, Vector Quantization, Pattern Recognition, PIBRAS.**

I. INTRODUCTION

The modern era revolves around recent advancement of technology in the development of smartphones and correlated growing request to gain access to the online services involving need of secure device verification. Recent methods for data safekeeping involves single level method (pattern based verification, static password, facial expression recognition, finger print recognition, retina scan etc.) for the user. The presented idea aims at the up gradation of the security methodologies by creating a guest user in the android environment and shielding the data by implementing some novel techniques such as speech recognition and PIBRAS. The guest user created in the proposed idea holds access to limited level of the device. The administrator user customizes the usage level for the custom user by exercising the administrator privileges. To ascertain himself as the administrator on the device, the user needs to get himself authenticated by a two level process. The first stage of verification of the user is the Speech Recognition process, followed by Pattern Recognition Based Authentication System.

A. *Speech Recognition Based Authentication System:* The Speech Recognition Based Authentication System is accomplished using Mel Frequency Cepstrum Coefficient (MFCC) and Vector Quantization[1]. The features are extracted from the speech signal using the MFCC method. The working of MFCC is dependent on the Fast Fourier Transform (FFT) value and the Discrete Cosine Transform (DCT) value of the speech signal. The amplitude computed by the DCT is taken as the cepstral coefficient. The speech signals are matched with the template on the basis of Vector Quantization and Euclidean Distance. The decision of whether authenticating the user to access the device is based on the difference of the Euclidean Distance between the input speech signal and the signal stored in the database template.

B. *Pattern Recognition Based Authentication System:* The second stage of authenticating the administrator user on the device is Pattern Recognition Based Authentication System. This method of verifying the user is an old yet promising technique. The user is required to provide an easy-to-remember yet a highly difficult-to-breach pattern. The template pattern design delivered by the user is stored in the database of the device for future references at the time of user verification. In this technique, the grid of pixels can either be a 3x3 grid or a 4x4 grid depending on the choice of the user. In the course of storing the template design or while verifying himself, the user can traverse through any particular pixel only once. Generally pattern lock is a set of gestures that phone user performs to unlock his smartphone when he needs to use it. It seems to be complicated, but actually it is not. A user has several points to create a 'unique' pattern which he finds easy to memorize and quick to draw so as to avoid shoulder surfing and other security breach attacks. The minimum number of points in the pattern to be traversed for a valid pattern is 4.

C. *Text Based Authentication Methodology:* The oldest yet one of the most secure method of authenticating the user is text based authentication. This method is more popular because it is difficult to breach and is independent of various environmental factors such as light, noise, dirt, moisture etc. It only needs the validation text and that doesn't get hampered by these factors. The text based approach works in two fields i.e. User Name and Password. These fields are the ID Credentials for the user and must be kept confidential by the user. The credentials entered at the log in screen should follow the documentation criteria. The data entered is stored in the database of the device so that it can be used at a later stage when the user tries to gain access and exercise the limited access level to the device as set by the administrator.

D. *Pixel Identification Based Registration and Authentication System:* The Pixel Identification Based Registration and Authentication System is a novel idea to authenticate the user in a very short span of time. Since the execution time of this method is very less so it reduces its complexity. This method is a Knowledge Based Authentication which is classified under the Recall Based Technique. This routine is even more stress free than the contemporary methodologies.

The user when registers himself, selects a particular pixel on the random image displayed on the log in screen. The pixel being displayed on the log in screen when the user selects it, is the access credential for him in this case. This pixel value is stored in the database.

II. RELATED WORK

With the advancement of technology and progress of science, almost every kind of transaction is possible now on smartphones. Moreover it is becoming a mini hayloft for any kind of documents. Thus a small security breach to the device poses a heavy threat to the confidential information and the stored documents. As a result, new methods to secure the device are designed. Device Authentication Techniques is the benchmark of device safekeeping. The term "Authentication" is derived from the Greek word **αὐθεντικός** meaning real or genuine and **αὐθέντης authentes** meaning author. It is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, or ensuring that a person is the same which he is claiming to be. Authentication often involves verifying the validity of at least one form of identification. It is a multi-factor process to validate the person.

Table 1. Categories of Authentication [2]

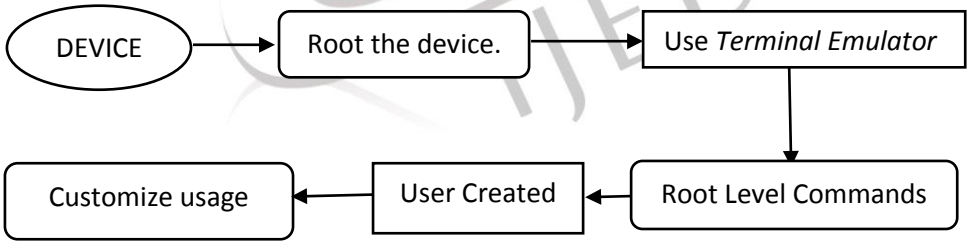
CATEGORIES	FACTORS	ELUCIDATION
PASSWORD	Knowledge	It is a knowledge based method of authentication. In this kind, the user is required to know the log-in credentials.
BIOMETRIC	Identity	This method of verification is based on the identity of the user. Distinctly featured human body parts are scanned to identify the user.
TOKEN	Possession	It is a possession based technique of authentication. In this methodology, the user is required to have the token to generate the pass code.

The elementary necessity for an authentication technique is that the password or the login testimonial should be easy to remember and recall. Moreover it should not be an easy target for security breach attacks. The proposed idea to safeguard the device and the records stored is to bifurcate the user access level. This bifurcation would shield the device to a higher extent as the custom user, who is the only other valid user to access the device will not be able to traverse through the device with organizational privileges.

III. PROPOSED METHODOLOGY

The proposed knowledge is based on limitation of the access rights on the device. The smartphones normally have an administrator user which has the license to access the complete device and navigate through all the stored records. This can be a major threat to the security of the important Electronic Data as any of the user who accesses the device has the freedom to view and modify the stored records. So, to enhance the safekeeping, the following is proposed to be executed on the device:

A. *Creating a custom level user*: The first step of the proposed idea is to create a guest user in the android environment. Technically, this process revolves around changing the boot level background in android. This can be done by rooting the phone and then using *Terminal Emulator* on the device. This would help the user to visit a new screen at every instance of login phase. The device can have a custom user by following the below given steps.



Once the administrator exercises Terminal Emulator, then he just needs to use several root level commands to create the custom user on the device.

B. *Authentication Proposition:* In present time, the smartphones manufactured have a single level authentication system for the user to log-in. The authentication schemes utilized are satisfactory but individually does not hold high level of security to the device. To overcome the slight probability of device security breach, the paper proposes to implement several novel method of device safe keeping along with several old but successful methods. The proposed idea is to have a multi-level authentication scheme for both the administrator and the created custom user on the device. This mode of verifying the user will enhance the safeguarding of the stored documents. The steps of authenticating the administrator on the device are:

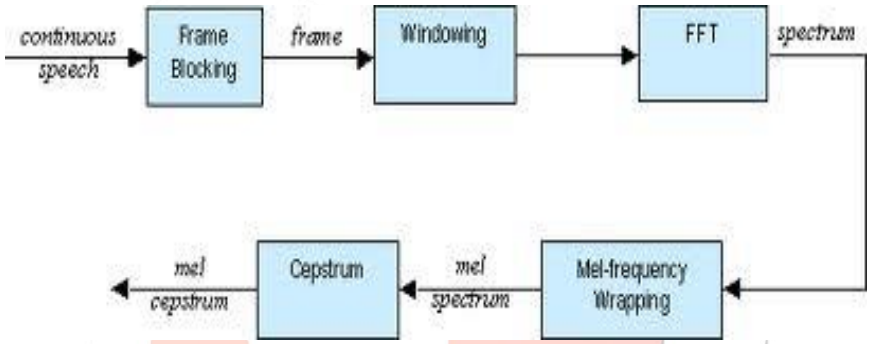
1) *Speech Recognition Based Authentication System:* The speech recognition based user authentication methodology is a novel approach for enhancing the security. This is so, because it involves the extraction of various features of the speech signal being processed. This approach identifies the user by distinguishing him on the basis of the extracted features

from the voice signal fed into the device and identifying him on the basis of the Vector Quantization and the difference in the Euclidean Distance of the signal and the template. The features can extracted from either Mel Frequency Cepstrum Coefficient (MFCC) or Linear Predictive Cepstrum Coefficient (LPCC). Although, studies have established that the former is more robust and efficient as compared to the latter. This approach is accomplished in following steps:

a. Signal Procurement: To start the speech recognition process, the voice signal is fed into the device using a microphone. The signal is converted to digital form for further execution. The accuracy of the process depends on the frequency and duration of the attained signal.

b. Signal Filtration: The input signal is a combination of speech traces along with some void time instances. The accuracy of the speech recognition system is inversely proportional to the void instances in the signal. Here the signal is filtered from such instances and is segmented into distinct frames which expand up to several milliseconds (preferably 25 ms). The segmented signal provides more accurate feature extraction results as it contains only the speech signals.

c. Feature Extraction: Feature extraction is one of the most vital step of this methodology. The distinct features of the input signals are extracted on the basis of the speech signal preprocessing to develop a template to be stored in the database. Under idealistic conditions, this process is robust to the inherent capriciousness of the human speech. To obtain the features from the signal, a number of methods can be implemented. Two of the most successful methods are Linear Predictive Cepstrum Coefficient (LPCC) and Mel Frequency Cepstrum Coefficient (MFCC). MFCC[3] is preferred because it is more robust and effective as compared to other methods. MFCC works as accordance to the given figure.



The result of this step are plotted linearly if the frequency of the signal is below 100Hz or if frequency is greater than 100Hz then it is plotted logarithmically. The plot is converted to time domain by

$$Mel(f)=2595*\log 10\ (1+f/700)$$

d. Signal Modelling: After the features are extracted from the speech signal, the corresponding template undergoes a training phase. For this, Vector Quantization[4] is implemented as it allows to define the speech signal by a vector of predefined size after the signal is clustered. This method works on the basis of LBG algorithm thus is more cost effective. The centroid obtained to be registered in the code book are used to design the template for the process. These templates are used at the verification step to calculate the Euclidean distance between the input and stored template to provide the threshold distance. It works on the principle of block coding. Each centroid represents a miscellaneous class of speech signal which is significantly compressed. Each divided frame is called a region and its center is named as Code Word.

The above mentioned steps form parts of the Registration phase and the Verification phase. In the registration phase, the result of the above mentioned steps are used to make the template. While in the verification step, after the speech signal undergoes MFCC and Vector Quantization, the distance metric is computed from the obtained coefficients. The obtained metric is used for verification. The Euclidean Distance is calculated by given law,

$$d(p,q) = d(q,p) = [(q_1- p_1)^2 + (q_2-p_2)^2 +\ldots\ldots\ldots\ldots+ (q_n-p_n)^2]^{1/2}$$

Let MFCC(n; p) be the MFCC coefficients of a given user and V Q(n; q) the query reference model, p >> q:

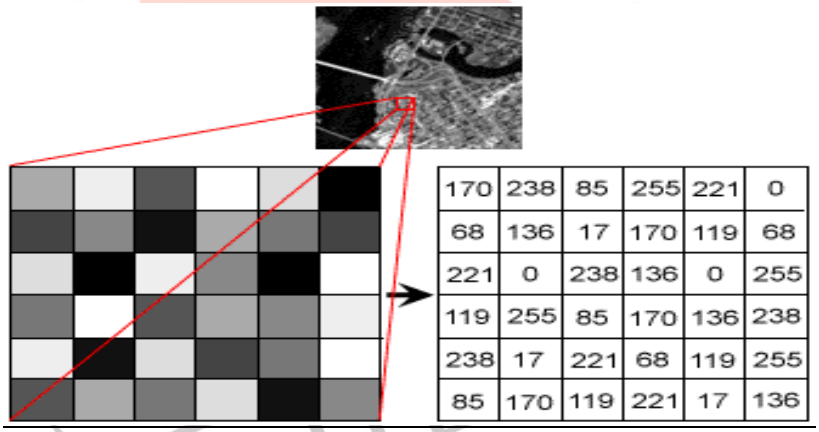
$$MFCC=\begin{bmatrix} MFCC_{11} & MFCC_{12} & ::: & MFCC_{1p} \\ MFCC_{21} & MFCC22 & ::: & MFCC_{2p} \\ & \vdots & & \\ & \vdots & & \\ MFCC_{n1} & MFCC_{n2} & ::: & MFCCnp \end{bmatrix} \qquad VQ = \begin{bmatrix} VQ_{11} & VQ_{12} & ::: & VQ_{1q} \\ VQ_{21} & VQ_{22} & ::: & VQ_{2q} \\ & \vdots & & \\ & \vdots & & \\ VQ_{n1} & VQ_{n2} & ::: & VQ_{nq} \end{bmatrix}$$

The authentication is successful only if the computed Euclidean Distance is lower than the provided threshold frequency.

2) *Pattern Recognition Based User Authentication:* Pattern based authentication technique is an old yet one of the most secure mode of securing the device against the security breaches. This method is based on the Point-Of-Interest being displayed on the log-in screen. This method works in two stages i.e. Registration and Verification. In the first stage, the user traverses through the grid of POI to form a unique pattern which is stored as the prototype. In the verification stage, the input pattern is compared with the prototype to grant or deny access to the user. This method is successful because the Lock sequence is encrypted with a SHA1 hashing algorithm. Since SHA1 is a one-way algorithm there is no reverse function to convert hash to original sequence. To restore the code the attacker will need to create a table of sequences with hash strings which proves to be a tedious job.

3) *Text Based User Authentication:* Text based user authentication is the oldest form of verification process. This method is based on text string entered by the user on the device. It has two fields to execute namely User Name and Password. The string entered should satisfy the two basic needs of authentication system i.e. i) It should be easy to recall ii) It should be resistant to breach attacks. So the user should not enter any string which should be very easy to be breached, moreover it should not be highly difficult because as a result of tough credentials, the user will not be able to memorize it easily and will make a note of it somewhere. This will add another dimension to security attack on the device.

4) *Pixel Identification Based Registration and Authentication System:* PIBRAS[5] [6] is another novel authentication method proposed in the paper. This approach revolves around selecting the same pixel on the displayed random image on the login screen. When the user attempts to access the device, a random image is displayed on the login screen. Since an image is a collection of pixels, the pixel value of each coordinate of the image is computed by the device. This is done by the Image Compression Technique. Studies have shown that the Loco-I Image Compression Algorithm is one the most effective and precise approach for calculating the pixel value of the image as it is a lossless algorithm. In the registration phase, the user selects the pixel of his choice from the displayed image as a result of which the computed pixel value is displayed to him. This pixel value is the confidential login credential for the user.



170	238	85	255	221	0
68	136	17	170	119	68
221	0	238	136	0	255
119	255	85	170	136	238
238	17	221	68	119	255
85	170	119	221	17	136

In the verification phase, the user is displayed the same image as he gets himself authenticated in the Tier-I level of security through the Text Based Authentication System. Thus the same pixel value or the quantitative value is required to be selected by the custom user in order to access the device as the guest user level and exercise the limited access.

IV. CONCLUSION

User authentication is the fundamental step for securing the confidential information in most of the device security contexts. To enhance the security mechanism, the user level is bifurcated with change in the access level depending on the user level. Moreover, the user authentication is proposed to be more sheltered by a concatenation of novel and existing methods. The multi factor authentication system reduces the probability of security breaches and protects the device from illegal access.

REFERENCES

[1] M. Baloul, E Cherrier, C Rosenberger. *Challenge Based Speaker Recognition For Mobile Authentication*. International Conference of the Biometrics Special Interest Group, 2012

[2] http://ict.govt.nz/guidance-and-resources/standards-compliance/authentication-standards/guidance-multi-factor-authentication/3-factors-authenticati/

[3] Prof. Ch. Srinivasa Kumar, Dr. P Mallikarjuna Rao.*Design Of An Automatic Speaker Recognition System Using MFCC, Vector Quantization and LBG Algorithm*. International Journal on Computer Science and Engineering, Vol 3 No. 8, August 2011.
[4] Singh Satyanand, Dr. E.G. Rajan. *Vector Quantization Approach For Speaker Recognition Using MFCC and inverted MFCC*. International Journal Of Computer Applications, Vol. 17, No.1, pp.1-7, March 2011.
[5] V Priya Dharshini, A Gomathi, N Saravanaselvam. *A Novel Based Multi level Graphical Authentication System*. International Journal Of Advanced Research In Computer and Communication Engineering, Vol 2, Issue 9, September 2013
[6] Ahmed Almulhem. *A Graphical Password Authentication System*. 978-0-9564263-7/6/$25.00 IEEE 2011.