Semiconductor Optoelectronics
ISSN: 1001-5868

A NOVEL APPROACH TO AUTHENTICATE SMARTPHONES USING SEQUENCE OF MULTIPLE MULTIMEDIA FEATURES FOR ROBUST AUTHENTICATION

Shiva Prasad M S
1Research Scholar, Department of Studies in Computer Science, Davangere University- 577007 India

Chandrakant Naikodi
2Associate Professor and Chairman, Department of Studies in Computer Science, Davangere University- 577007 India

Abstract: Smartphone authentication is essential for securing sensitive data even though applications have implemented their safety measures. Since it is the first step towards entering the system, a robust authentication process is needed. We propose a smartphone authentication based on a Sequence of Multiple Multimedia Features (SMMF), which encompasses various authentication techniques including pattern recognition, face recognition, password, OTP, Sequence of Multiple Fingerprints (SMF), and other features detailed in this paper. We have implemented this technique using an appropriate algorithm as outlined in our methodology. Furthermore, we have evaluated by calculating the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Additionally, ROC curves with AUC values are generated, utilizing parameters such as true positives, true negatives, false positives, and false negatives. This evaluation involved the utilization of True Positive Rate (TPR) and False Positive Rate (FPR) equations and with the help of the above-mentioned parameters, the probability of success and failure rates are calculated using combination equations.

Keywords: SMMF, SMF, FAR, FRR, Accuracy, True Positive, False Positive, True Negative, False Negative.

Introduction

Smartphone usage is increasing day by day and authentication techniques are also evolving with usage, for example, Google and Baidu provide voice authentication for its Android operating system [1]. Even after improvements in smartphone authentication, it is projected that four out of ten phones are under intrinsic cyber-attack [2]. Smartphones use stored information to authenticate user and entry point authentication and these methods are not sufficient to secure sensitive data. Implicit or continuous authentication is the current trend in user authentication for smartphones to fix such issues [3]. The smartphone uses biometrics and other multimedia behavioral features to authenticate the system or applications of a smartphone. Many multimedia features, including fingerprint, iris, face, voice, and others, have been deployed individually for authentication. Some features are intrusive to users because they need to participate in gathering data and because they are easily vulnerable to attack when they are verified individually [4]. We are presenting a combined approach that can be integrated with the Sequence of Multiple Multimedia Features (SMMF) and Sequence of Multiple Fingerprints (SMF) as shown in Figure 1.

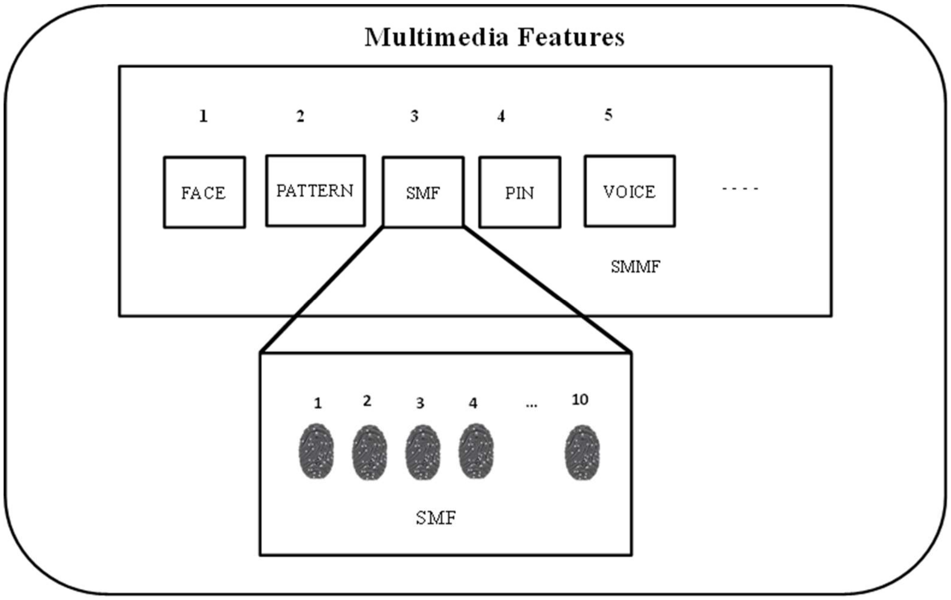

Figure 1: SMMF Architecture

The idea is to combine individual multimedia features in sequence by allotting each feature a Unique Identification Number (UID) that serves the authentication process in a specified order. Table 1 illustrates all possible Multimedia Features the user can configure while registering to a smartphone and the user can assign each feature with proper sequence value. The user must provide the registered features one by one, the model provides a login success message only after successful attempts from all the sequences provided, if any one feature fails to recognize the user then authentication will fail. In addition to this, a model is integrated with SMF and it can be added to any sequence of the UID making it a subset of SMMF as shown in Figure 1. Here fingerprints for SMF need to be registered separately discussed in [13] and the main reason to use fingerprint as SMF is that in addition to being used to unlock smartphones, fingerprint recognition is also used to activate other security-related features, such as authorizing transactions in banking applications and also the success rate of fingerprint authentication is high when compared to other techniques [6] [7].

To understand the working of the model let us consider an example in which the user registers Face, Password, Pin, Pattern, Voice, and SMF respectively in sequence as shown in Figure 2, while authenticating user must provide the registered features in the same order to get valid authentication, if any one feature is skipped or mismatched then it leads to failure as in Figure 3.

Sequence /UID	1	2	3	4	5	6	7	8	9
Features	👤	🔊	12345678	1234	⁘		5634	🔊	Screen Angles + Shaking Directions etc.

Name	Face	Voice	Password	Pin	Pattern	Fingerprint	OTP	Audio	Others

Table 1: Multimedia Features

The sequence applies not only for SMMF but also for fingerprints, if any one fingerprint turns invalid or changes its sequence within the subset, then the entire authentication shows invalid as in Figure.3.

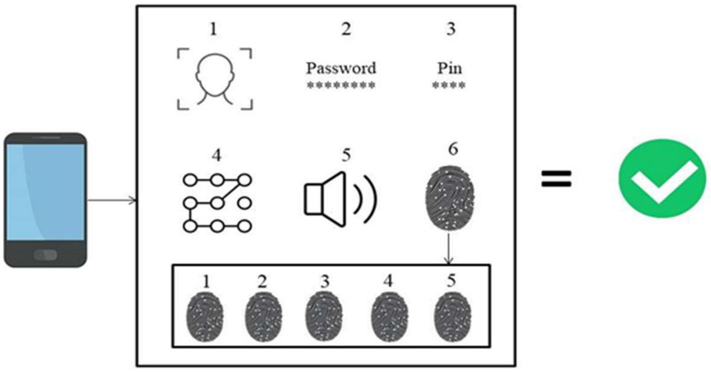

Figure 2: SMMF with Valid Authentication Sequence

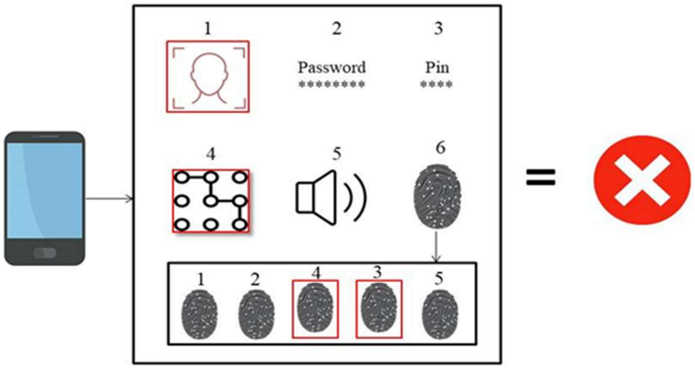

Figure 3: SMMF with Invalid Authentication Sequence

It shows three basic invalid scenarios at first, if Face recognition is not accepted for UID sequence 1 then entire authentication process will exit at first instance. Second, three sequences are authenticated as valid that is for Face, Password, and Pin but the Pattern is not matching for original data. Third, even if the entire SMMF feature authentication is valid but the fingerprint sequence in a subset is missing with its UID order or the user has swapped two fingers with 3 and 4 that also becomes an invalid authentication.

In this approach, users can register up to 10 fingers for the SMF authentication process for increased robustness. Thus integrating SMMF and SMF techniques at an operating system level for any smartphone becomes a robust authentication process. Several attacks such as Template matching, Shoulder surfing, and distortion attacks [8] [9] [10] can easily be overcome through this approach and it provides better assurance that the smartphone is in the hands of an authorized user.

Literature Review

As part of the literature review, we tried to provide all the latest developments and their corresponding future trends, Table 2 highlights the contributions of the different authors.

Sl.no	Reference Paper	Contribution/s	Future Enhancements
1	Dev.Nath et al. [11]	False Accept Rate (FAR) and False Reject Rate (FRR) are more in single fingerprint authentication that need to be minimized.	The error rates occur quite often and have to be reduced.
2	Zahid Akhtar et al. [12]	Touch stroke, phone movement, and face patterns can be used for smartphone authentication.	Implicit smartphone Multimodal biometric systems using touch stroke can be implemented on any smartphone.
3	Shiva Prasad MS et al. [13]	The sequence of Multiple fingerprints creates a robust authentication environment for smartphones.	It can be enhanced with other authentication techniques.
4	Chiara Galdi et al [14]	Multimodal authentication systems can be used to create better security for smartphones.	The potential to strengthen system defenses against assaults by including anti-spoofing techniques is still being researched.
5	Jie Chang et al. [15]	Excessive feature extraction leads to the low accuracy of the pattern recognition method.	Advanced techniques need to be identified.
6	Mariia Nazarkevych et al. [16]	Multimodal biometrics is mainly used for certification and identity verification.	Ateb-Gabor filters are becoming a traditional approach for biometric imaging.
7	Dindar Mikaeel Ahmed et al. [17]	Multiple biometric identification systems have advantages over single biometric identification systems.	Multiple fingerprints can secure a system more than a single fingerprint.
8	Gianmarco Baldini et al. [18]	Very high identification accuracy can be obtained in the electronic components using fingerprints.	Climate change must not affect the quality of fingerprint images.
9	Daniel Tordera et al.[19]	A solution to the problem of climate change factors by implementing organic photodetectors (OPD).	In the future OLED can be upgraded to other screens e.g.: AMOLED, QLED.
10	Nasir Memon et al. [20]	Fingerprint sensors have turned modern smartphones into miracles of convenience.	Master Prints need further security than it is now.

Table 2: Literature Review

Methodology

The proposed methodology presents the working model that combines SMMF and SMF authentication techniques and it can be implemented on an operating system of a smartphone provided with the interface to select a sequence to allocate for specific application/applications as shown in Figure 4. The SMF works as a subset to SMMF and the subset can be placed in any UID order to a created set and fingerprints are limited under the number of SMMF allocated. For example, if the intended number of sequence for authentication is 10 and SMMF is registered for the first 4 sequences then the SMF need to be registered for the remaining sequence which is 6 as shown in equation 1.

$$\text{Total Sequence} = \text{SMMF} + \text{SMF} \qquad (1)$$

The proposed method uses existing authentication techniques to create a robust system. A smartphone will be provided with an option to select an application to create a robust environment using SMMF.

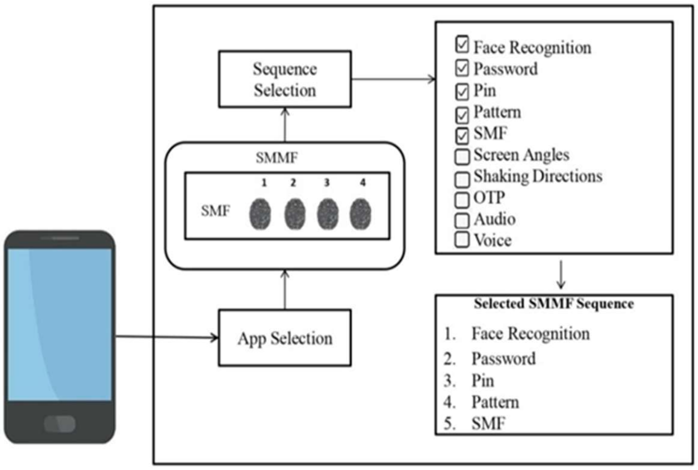

Figure 4: Working Flow of SMMF

Once the specific application is selected user will be provided with the list of multimedia features along with the SMF and a checklist needs to be provided to select a preferred authentication technique in sequence. A UID is generated upon selection of the sequence. The simulation model was designed using Android with the manual sequence generated as shown earlier in Figure 1. The maximum sequence intended to provide for authentication is up to 10 with a combination of SMMF and SMF as an option.

The simulation model designed uses the face recognition technique at the first sequence to authenticate a user and the face recognition algorithm uses modules: Face verification, Face detection, and Face analysis shown in Algorithm 1 each module results in a different statement depending on the recognition process and according to [21] face recognition model reaches up to an accuracy of 97%.

Algorithm 1: Algorithm on Face Recognition

Input: User face as image
Output: Face recognized or Not Recognized

```
# Face Verification
1. Verification = face.verify (img1_path = ‘image1.jpg’, img2_path = ’image2.jpg’)
2. Result = True or False

# Face Detection
3. Detection = face.find( img_path = ‘ image.jpg’, Db_path =  ‘db_image.jpg’)
```

```
4. Result = Found or Not Found

# Face Analysis
5. Analysis = face.analyze( img_path = ‘image.jpg’, actions = [“age”, “gender”,
“emotions”, “race”])
6. Result = actions
```

Patterns and passwords are widely used authentication techniques in any smartphone. Because of its non-behavioral characteristics, it is considered to be a simple technique to unlock the smartphone. The present smartphone uses the SHA-1 algorithm to encrypt the registered pattern and password values [22]. We have used this technique in our simulation model to add a certain level of security if it is used as a sequence within the SMMF approach. A model was designed to simulate SMF that uses a fingerprint sensor and the SMMF application is integrated to sequence both. Each fingerprint is assigned a UID that combines the sequence of authentication. The fingerprint sensor identifies the finger that is placed on a sensor by displaying its corresponding registered UID and the user must register his credentials on the application including the UID registered with the same sequence Algorithm 2 shows the working of SMF that matches the registered UID and user sequenced id value.

Algorithm 2: Algorithm on SMF

Input: Accept Fingerprint Sequence
Output: Login Success or Login Failed

```
1: Initialize a=0,b=0,c=0,d=0
2: if (Result_String1)  #verifying first sequence id
3: then a= a+1
4: else go to Step 19
5: if (Result_String 2) #verifying second sequence id
6: then b= b+1
7: else go to Step 19
8: if (Result_String 3) #verifying third sequence id
9: then c=c+1
10: else go to Step 19
11: if(Result_String 4) #verifying fourth sequence id
12: then d=d+1
13: if (d = = 1)
14: append string as Db_string #ex.”1234”
15: else go to Step 19
15: repeat steps 1 to 14 for other sequences if exist
16: log in with username and fingerprint sequence as Pwd_string
16: if Pwd_string = = Db_string
```

```
then
    Login Success
else
    Login Failed
end if
```

Fingers are scanned in sequence by generating UID for each fingerprint by using a fingerprint sensor. Fingerprint and finger ID are stored in memory which is capable of identifying finger ID once the registered finger is scanned. The user will be registering to the application with his credentials and user ID that are generated upon fingerprint registration. Multimedia features are authenticated in sequence as selected by the user from the control settings of the operating system. In this method, we have simulated the SMMF model manually with four multimedia feature sequences that are face recognition, password, pattern, and 4-digit pin. Each multimedia feature is authenticated individually, after every successful authentication a pre-programmed feature will be displayed for the next login. If all the multimedia features are authenticated successfully then the SMF authentication process begins as shown in Figure 5.

The SMF authentication technique appends both finger ID and user ID as a string value. To authenticate the algorithm that checks whether the finger ID matches with the user ID, if the match returns true then the complete system will be authenticated if any one sequence fails among SMMF or SMF then login will fail. Thus it creates a robust authentication process and it can be recommended to create an unbreakable environment for sensitive applications.

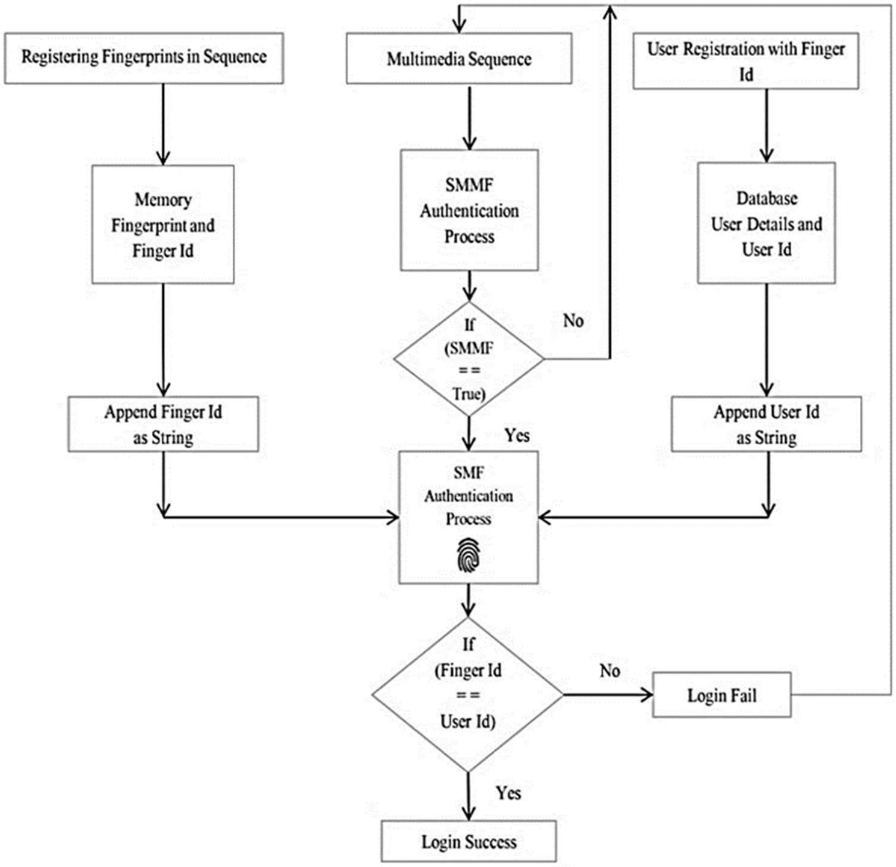
Registering Fingerprints in Sequence
Multimedia Sequence
User Registration with Finger Id
Memory Fingerprint and Finger Id
SMMF Authentication Process
Database User Details and User Id
If (SMMF == True)
No
Yes
Append Finger Id as String
Append User Id as String
SMF Authentication Process
If (Finger Id == User Id)
No
Login Fail
Yes
Login Success

Figure 5: Working Flow of SMMF and SMF

Experiment and Results

As the experiment was conducted individually for multimedia authentication and SMF on the simulation model, we were able to extract the False Acceptance Rate (FAR) and False Rejection Rate (FRR) for face recognition and fingerprint sequences. The ratio of false acceptances to the total number of test samples determined to be falsifications is applied to compute the false acceptance rate, or FAR and FRR is determined by splitting the number of test samples divided by the number of false rejections of registered users as referred in equation 1 and 2.

False Acceptance Rate = Number of False Accepted / Total Samples (1)

False Rejection Rate = Number of False Rejected / Total Samples (2)

We have registered a face, pattern, password, and 4-digit PIN in an order followed by 6 sequences of fingerprints for an authorized user, FAR and FRR were tested for face and fingerprint behaviors. At first, a registered user was made to scan his face upon face recognition several times and we got 0 false rejections SMF was tested for several attempts and the FRR readings are noted in Table 6. FAR is calculated by 10 different attempts by unregistered users selected randomly and tried to access the model as imposters and the readings of those attempts are also recorded in Table 6. An UID is registered for each authentication process for face recognition UID holds the value 1, password value 2, 4-digit pin value 3, pattern value 4, and SMF is registered from 5 to 10.

Predicted

	Actual	
Predicted	TP	FP
	FN	TN

Table 5.Confusion Matrix on Predicted and Actual Values

The Receiver Operating Characteristic Curve (ROC) with Area under the Curve (AUC) represents the performance of both SMMF and SMF with attributes of True Positive Rate (TPR) and False Positive Rate (FPR) as shown in Figure 6 using confusion matrix [23] consists of four parameters related to authentication as shown in Table 5. Includes True Positive (TP),

	Face Recognition	**Fingerprint Sequence**					
UID	1	5	6	7	8	9	10
FAR	0.1	0.2	0.3	0.1	0	0	0
FRR	0	0.2	0	0.2	0.1	0	0.1

Table 6.Results Obtained from Face Recognition and Fingerprint Sequence

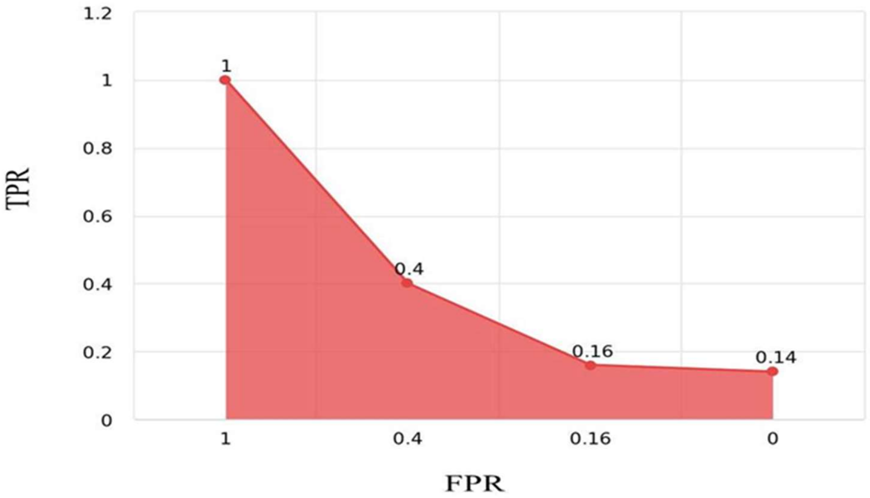

Figure 6: ROC Curve with AUC for SMMF and SMF Analysis

The ROC curve is computed with two parameters True Positive Rate (TPR) and False Positive Rate (FPR) refer to equations 3 and 4. Both the parameters are obtained with 4 different threshold values T0, T0.1, T0.2, and T0.3 using logical regression classifiers. For each threshold, the resultant TPR and FPR values are plotted on the graph i.e. T0 (1, 1), T0.1 (0.4, 0.4), T0.2 (0.16, 0.16), and T0.3 (0.14, 0).

i. False Positive Rate (FPR) also coined as Error Rate:

$$FPR = \frac{\text{FP}}{\text{FP+T}} \qquad (3)$$

FP = False Positive
TN = True Negative
(FP + TN) Indicates the Total Number of Negatives

ii. False Negative Rate (FNR) also known as Missing Rate because of missing True Positive condition by test result:

$$FNR = \frac{\mathrm{FN}}{\mathrm{FN+TP}} \qquad (4)$$

FN = False Negative
TP = True Positive
(FN + TP) Indicates the Total Number of Positives

iii. True Positive Rate (TPR) can be termed as Sensitivity Rate:

$$TPR = \frac{\mathrm{TP}}{\mathrm{TP+FN}} \qquad (5)$$

TP = True Positive
FN = False Negative
(TP+FN) Indicates the Total Number of Actual Positives

iv. True Negative Rate (TNR) termed as Specificity Rate:

$$TNR = \frac{\mathrm{TN}}{\mathrm{TN+F}} \qquad (6)$$

TN = True Negative
FP = False Positive
(TN + FP) Indicates the Total number of Actual Negatives

True Positive holds positive and the test predicts the Positive value, True Negative holds the actual value as negative and the test predicts negative, False Negative holds positive but the test predicts negative and False Positive holds negative value as actual but the test predicts positive value [23]. The ROC curve is plotted based on the calculations performed using these 4 authentication parameters. The other multimedia sequences such as Password, Pattern, and Pin (3P's) with assigned UID 2, 3, and 4 respectively have been tested based on usage speed versus time. We have conducted the experiment on a user, who made to register a new Password, Pattern, and Pin on the model. The initial time taken to match all three was recorded individually and the average authentication match for the day was calculated and the average match for 5 consecutive days was calculated considering it as a threshold value as shown in Table 7. If a user tries to log in with more threshold time then it can be considered as imposter access.

	Average Per Day (in Sec.)					**Overall Average (in Sec.)**
Days	**D1**	**D2**	**D3**	**D4**	**D5**	**Threshold**
Password	5	5.2	4.8	4.4	4.2	4.7
Pattern	2.6	2.6	2.8	2.2	2	2.44
Pin	2.6	2.4	2.4	2	1.8	2.24

Table.7.Average Threshold Values

The accuracy of the authentication model is computed upon 4 parameters that are TP, TN, FP, and FN as we have analyzed the authentication process for 5 days for 20 different users and recorded the true and false rates shown in Table 8. As the users authenticated to the model it was observed that accuracy kept increasing as shown in Figure 7. The accuracy is calculated based on equation 7 [24]. As the user became familiar with the model it was observed that the false negative rate was decreasing that helped in the increase of accuracy of the system.

$$Accuracy = \frac{\sum TP \quad \sum TN}{\sum TP+\sum TN \quad \sum FP+\sum FN} \qquad (7)$$

Days	TP	TN	FP	FN	Accuracy (%)
Day 1	19	27	16	2	71
Day 2	25	24	14	2	75
Day 3	28	21	13	2	76
Day 4	32	20	13	1	78
Day 5	33	19	11	1	81

Table 8: Accuracy Level of SMMF System

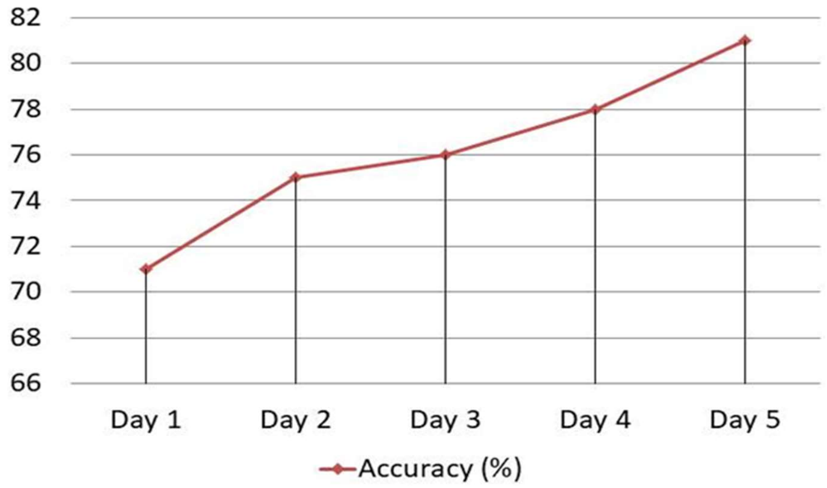

Figure.7. Accuracy Rate of Authentication Model

The probability of FAR and FRR can be calculated using equation 8 and 9. It provides a probability solution using combinations indicated as C (n, k) where ‘n’ is the total number of unauthorized users and ‘k’ is the number of users incorrectly accepted. FA is a ratio of False Acceptance towards misclassifications. CR is the probability of Correctly Rejecting unauthorized users.

$$P(FAR) = \{C(n,k) * P\,(FA)^{K} * P(CR)^{n-k}\} \quad (8)$$

The probabilistic analysis was conducted on 10 different unauthorized users out of which we got 2 misclassifications of falsely accepted users i.e. n is 10 and k is 02. FAR value is calculated to be 0.0187 which means 1.87 % is the chance of the system accepting the unauthorized user as valid during the entire SMMF authentication process.

$$P(FRR) = \{C(n,k) * P\,(FR)^{K} * P(CA)^{n-k}\} \quad (9)$$

The probabilistic analysis was conducted on 10 different unauthorized users out of which we got 1 misclassification of falsely rejected user i.e. n is 10 and k is 01. FRR value is calculated to be 0.18 which means 18 % is the chance of the system rejecting the authorized user as invalid during the entire SMMF authentication process.

Conclusion

Our research introduces a comprehensive smartphone authentication method based on SMMF. This approach combines a range of authentication techniques, including pattern, face recognition, password, OTP, SMF, and other features discussed in this paper. We have successfully implemented this method, employing an appropriate algorithm as detailed in our methodology.

To assess the effectiveness of our approach, we conducted a thorough evaluation, which involved calculating key metrics such as False Acceptance Rate (FAR) and False Rejection Rate (FRR). Additionally, we generated Receiver Operating Characteristic (ROC) curves and determined the Area under the Curve (AUC) values. This evaluation employed essential parameters including true positives, true negatives, false positives, and false negatives, allowing us to assess the performance of our authentication method by utilizing True Positive Rate (TPR) and False Positive Rate (FPR) equations. The probability of our model showed 98.13% and 82% accuracy respectively on FAR and FRR. Our findings provide valuable insights into the viability and security of our proposed smartphone authentication method.

References

- Wu, Libing, et al. "LVID: A multimodal biometrics authentication system on smartphones." IEEE Transactions on Information Forensics and Security 15 (2019): 1572-1585.
- Oludayo, Ogundele Israel, et al. "A Review of Smartphone Security Challenges and Prevention." International Research Journal of Innovations in Engineering and Technology 7.5 (2023): 234.
- Rayani, Praveen Kumar, and Suvamoy Changder. "Continuous user authentication on smartphone via behavioral biometrics: a survey." Multimedia Tools and Applications 82.2 (2023): 1633-1667.
- Qin Zou, Yanling Wang, Qian Wang, Yi Zhao, Qingquan Li. “Deep Learning-Based Gait Recognition Using Smartphones in the Wild.”, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2020.
- Shen, Zhihao, et al. "IncreAuth: Incremental Learning based Behavioral Biometric Authentication on Smartphones." IEEE Internet of Things Journal (2023).
- Jo, Young-Hoo, et al. "Security analysis and improvement of fingerprint authentication for smartphones." Mobile Information Systems 2016 (2016).
- Oogami, Wataru, et al. "Observation study on usability challenges for fingerprint authentication using WebAuthn-enabled android smartphones." Age 20 (2020): 29.
- Wilson, Charles L., et al. (2004). Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. US Department of Commerce, National Institute of Standards and Technology.
- Adebimpe, Lateef Adekunle, et al. "Systemic Literature Review of Recognition-Based Authentication Method Resistivity to Shoulder-Surfing Attacks." Applied Sciences 13.18 (2023): 10040.
- Bâce, Mihai, et al. "PrivacyScout: Assessing Vulnerability to Shoulder Surfing on Mobile Devices." (2022): 650-669.

- Dev.Nath.; Saurav Ray.;Sumit Kumar Ghosh. Fingerprint Recognition System: Design & Analysis.2011
- Akhtar, Zahid, et al. "Multimodal smartphone user authentication using touchstroke, phone-movement and face patterns." 2017 IEEE global conference on signal and information processing (GlobalSIP). IEEE, 2017.
- Shiva Prasad MS.;Chandrakanth Naikodi. "A Novel Approach to Login Smartphones Using Sequence of Multiple Fingerprints for Secured Authentication". 2023. Journal of Harbin Engineering University ISSN: 1006-7043.
- Galdi, Chiara, Michele Nappi, and Jean-Luc Dugelay. "Multimodal authentication on smartphones: Combining iris and sensor recognition for a double check of user identity." Pattern Recognition Letters 82 (2016): 144-153.
- Jie Chang.; Xiaojun Zuo.; Botao Hou.; Shuo Liu. Mobile APP fingerprint feature. 2021 extraction pattern recognition based on Random Game.2021.
- Mariia Nazarkevych .; Natalia Kryvinska.; Yaroslav Voznyi. Applying Ateb–Gabor Filters to Biometric Imaging Problems. 2021
- Dindar Mikaeel Ahmed.;Siddeeq Y. Ameen.; Naaman Omar.;Shakir Fattah Kak.; Zryan Najat Rashid.;Hajar Maseeh Yasin.;Ibrahim Mahmood Ibrahim.; Azar Abid Salih.;Nareen O. M.Salim .; Awder Mohammed Ahmed. A State of Art for Survey of Combined Iris and Fingerprint Recognition Systems. 2021
- Gianmarco Baldini, member, IEEE and Gary steri. A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components. 2017
- Daniel Tordera, Bart Peeters; Hylke B. Akkerman; Albert J. J. M. van Breemen; Joris Maas; Santhosh Shanmugam; Auke J. Kronemeijer; Gerwin H. Gelinck. A High-Resolution Thin-Film Fingerprint Sensor Using a Printed Organic Photodetector. 2019.
- Nasir memon.; Aditi Roy.; Arun Ross. That Fingerprint Sensor on Your Phone Is Not as Safe as You Think.2017.
- Face recognition Algorithm : https://viso.ai/computer-vision/deepface/
- https://www.forensicfocus.com/articles/android-forensics-study-of-password-and-pattern-lock-protection/
- https://www.split.io/glossary/false-positive-rate/
- Agrawal, Arpit, and Ashish Patidar. "Smart Authentication for smartphones." International Journal of Computer Science and Information Technologies 5.4 (2014): 4839-4843.