*Journal of Harbin Engineering University* Vol 44 No. 7
*ISSN: 1006-7043* July 2023

# A Novel Approach to Login Smartphones Using Sequence of Multiple Fingerprints for Secured Authentication

**Shiva Prasad M S**[1]
[1]Research Scholar, Department of Studies in Computer Science,
Davangere University- 577007 India
shvprsdms@gmail.com[1]

**Chandrakant Naikodi**[2]
[2]Associate Professor and Chairman, Department of Studies in Computer Science,
Davangere University- 577007 India
chandrakant.naikodi@yahoo.in[2]

**Abstract**
The prevalence of smartphones is increasing rapidly and the majority of them employ fingerprint recognition as a method to authenticate any application, from login to financial transactions. Presently smartphones validate phone unlocking and other applications that safeguard the smartphone with a single fingerprint recognition technique. Yet, a single fingerprint might provide an imposter easy access to carry out the attacks on stored templates and also due to False Accept Rate (FAR) and False Rejection Rate (FRR). It is necessary to have the next security level for smartphones to strengthen the existing technique. One such method is implemented by employing multiple fingerprints processed in a registered sequence. This paper proposes SMF technique to provide strong authentication security to reduce the FAR rate and results are compared with the single fingerprint authentication. Experimental results are analyzed with ROC curves by computing it with true positive and false positive rates and we have computed that how SMF technique is secured and robust on template attack using combinations. Results are discussed based on accuracy, robustness and speed using enhanced equations and performance is compared with existing system.

**Keywords**: SMF, UID, Imposters, Fingerprint Sensor, Security and Robustness.

## 1. Introduction

Security is the main criteria in smartphone-connected devices. Smartphones use multiple security techniques such as face recognition, patterns, passwords, and fingerprint techniques for authentication [2] [10]. Among these techniques, fingerprint recognition is widely used due to its usability and ease of access in terms of providing high security. "Two like fingerprints would be found only once every $10^{48}$ years" [10]. But fingerprint techniques can also be compromised to several attacks according to [24] fingerprint recognition system can be attacked in 3 ways: Attack on sensor, Attack on communication channel and Attack on feature extractor module. Fingerprint sensors include four stages: Fingerprint sensing, Feature extraction, Image pattern matching, and decision making [21]. We are introducing an approach Sequence of Multiple Fingerprints (SMF) that can enhance smartphone security as we discuss in detail in the paper. For authentication, user uses a fingerprint sensor to match his/her fingerprint with the stored template or an image. According to [23] fingerprint authentication has low risk level but vulnerabilities do exist if we continue to use single factor authentication [24] through brute-force attack [2]. As smartphone usage is increasing rapidly security threats are also increasing day by day, so we need stronger security techniques that control the security breach because attackers are finding a way to violate the authentication either by hardware or software vulnerabilities [25] [26].

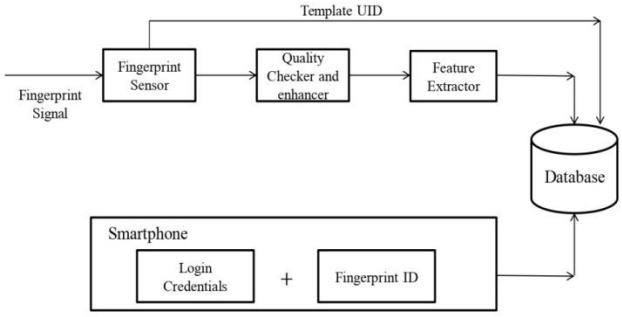


Figure 1: General structure of fingerprint Authentication

A Fingerprint template may be stolen and replayed, or it can be replaced in a system database by an impostor's template [17]. Single fingerprint authentication leads to a substantial increase in false acceptance rate (FAR) [18]. As the attacks may be possible and the problem with a single fingerprint is, it does not have combinations that trick the attackers and once a single fingerprint data has been compromised, it is compromised forever [12]. Implementing SMF increases the robustness level in overall authentication process and the general structure SMF is shown in Figure 1. If any one fingerprint is altered or misses the sequence then authentication will be failed because the algorithm matches sequence of fingerprints in a specific order of an authorized user, this reduces the chances of false acceptance rate, and the implemented application works only on SMF as registered as shown in Figure 2.

Distinct values are assigned for the user and the fingerprint as shown in Figure 2 if the user registers his fingers in the order of 1,2,3,4 then while authenticating he must have provide the same sequence if any one sequence is missed then authentication will be failed. SMF system is very efficient as a data will possess an Unique Identification Id (UID) to each fingerprint. The model has an integrated mobile application that allows users to log in. However, we have chosen a fingerprint sensor to authenticate smartphones rather than the fingerprint sensor on a smartphone [5] [7].

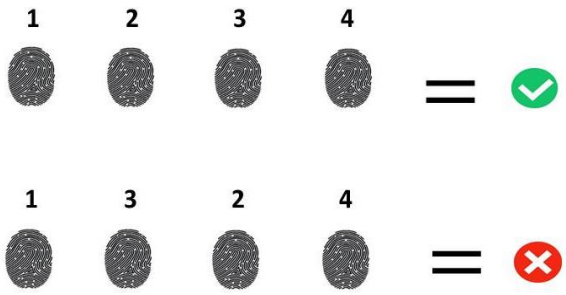


Figure 2: Authentication Process of SMF

The approach can increase robustness by making several successful attempts that enhances the fingerprint templates quality as we have conducted the experiment on SMF the failure rate became low. The model was developed using fingerprint sensor due to the requirement of a UID for each authentication. The application was intended to be built on a smartphone due to the limitations imposed by a Trusted Execution Environment (TEE) [5] [7]. We have designed it using a fingerprint sensor that is then integrated with the mobile application. Each fingerprint is registered and stored on the database with the UID assigned to all the registered fingerprints of a user and each user can register up to ten fingerprints. Once the fingerprint is registered, a unique value is assigned to each fingerprint. The user can register any number of fingerprints below ten. The user must scan their fingerprint in the order of registration while authenticating. The accuracy and robustness can be enhanced further if the designed model is built completely on the smartphone as part of operating system.

## 2. Hardware and Software Used

This paper is implemented using multiple hardware and software components. Some of the components are listed below.

i. Node MCU:

A development board and open-source firmware called Node MCU is based on the well-known ESP8266 Wi-Fi module. It offers a platform for creating Internet of Things (IoT) projects and applications. Because the Node MCU firmware is built on the Lua scripting language, interacting with the hardware is simple.

ii. OLED Display**:**

A 0.96-inch, 128X64 high-resolution display is incorporated within the OLED 0.96-inch monochrome graphic display module. Even without lighting, OLED 0.96 inches can function. OLED displays have stronger contrast than LCDs when the room is dark.

iii. Fingerprint Sensor:

High-precision, high-performance matching algorithms, and a high-capacity memory chip make up the R305 biometric fingerprint module. It operates by processing fingerprint image data, matching data, searching data in memory, and carrying out specified operations. While recognizing a person, the user can configure the module in 1:1 or 1: N mode and save the fingerprint data. A 3V3 or 5V microcontroller may directly connect with the fingerprint module. The R305 communicates with the microcontroller through serial communication. It is not feasible to alter the 57600 Baud Rate that is used by default.

iv. Push to On Button:

It is a button used to actuate the internal switching mechanism. They are operated manually and the size will vary depending on the component they come in a variety of shapes, sizes, and configurations.

v. Android Studio:

We can create apps for Android phones, tablets, Android Wear, Android TV, and Android Auto using Android Studio, which offers a single development environment. We may break our project into functional parts with structured code modules so that you can build, test, and debug each one separately. Everything that defines the workspace for an app in Android Studio is contained in a project, including source code, assets, test code, and build options.

## 3. Literature Review

As part of the literature review, we tried to provide all the latest developments and their corresponding future trends, following Table 1 highlights the contributions of the different authors.

As per the literature survey conducted by us, there is evident proof that the fingerprint is an efficient technique to secure a smartphone compared to other techniques such as face recognition, pattern, and password however attempts are made to break the existing system hence providing robust security is essential. So we require an enhanced technique to make the fingerprint to be more robust and secure. Some of the studies [3] [5] covered various applications, methods, and security goals in fingerprint recognition. Some of these surveys [2] [6] [9] have proposed architecture and working procedures of different fingerprint techniques. Few surveys [1] [13] [5] [7] discussed the problem and errors that are occurred while implementing fingerprint techniques.

## 4. Methodology

The simulation was designed with fingerprint sensor and an application that authenticates user using SMF that uses an algorithm shown in Table. 2. The device is powered using a micro USB and the sensor that identifies the fingerprints by assigning each finger with a Unique Identification (UID) number and that can store up to 127 fingerprints in its memory [27]. The fingerprint sequence is accomplished by the UID generated by fingerprint sensor. Figure 3 shows fingerprint sensor with other components and markings are described. The fingerprint sensor can distinguish SMF and user can assign any unique number to any of the finger shown in Figure 4 and as the user register he/she can use different fingers matching to incremented value generated. So when user tries login to system he/she must provide the same sequence of fingers as registered. Figure 5 shows the UID allotted to each finger on the OLED display provided with the fingerprint sensor in the registration process.

In the process of fingerprint recognition if registered finger is scanned, sensor recognizes its unique number assigned. The sensor uses WiFi for connecting to the database using node MCU. An application is designed to provide the interface for users to login and register with login credentials including fingerprint id.

**Table 1**: Literature Review of Related Work

| Sl.no | Reference Paper | Contributions | Limitations |
|---|---|---|---|
| 1 | Hanyung Junget et al. [1] | The importance of biometric authentication in mobile devices has been increasing owing to its excellent security and convenience. | The image of fingerprint ridges and valleys was also obtained using the OLED light source, but its contrast ratio is lower compared with that of QLED. |
| 2 | Israel Martin-Escalona et al.[2] | Fingerprinting solutions have been suggested and are expected to provide more stable measurements compared to using the RSS. | The three main issues of fingerprints are database construction, maintenance, and variability in observation. |
| 3 | Abdullah Saud et al. [3] | The discovery of fingerprints can be used in various applications like authentication methods, criminal search, and various security issues. | When the image quality was low, the features extracted could be distorted and untrue. |
| 4 | Mohamed Sabt et al.[4] | A TEE is a secure, integrity-protected processing environment, consisting of memory and storage capabilities | However, TEE still lacks a precise definition as well as representative building blocks that systematize its design |
| 5 | Jie Chang et al. [5] | A fingerprint feature extraction pattern recognition method based on a random game is proposed for mobile apps. After the fingerprint image processing, the fingerprint features in the image are extracted | The traditional feature extraction method for pattern recognition increases the computational complexity of the recognition method due to the excessive feature extraction, which leads to the low accuracy of the recognition method. |
| 6 | Marcel Busch et al. [6] | TEEs are an integral part of the security architecture of mobile devices. They provide an execution context where security-critical services, such as user authentication, mobile payment, and digital rights management | The correct implementation of a TEE is complex and comparable to the design of an operating system, posing innumerable challenges for vendors. |

| | | | |
|---|---|---|---|
| 7 | Ibrahim Jawarneh et al.[7] | Different categories of the arch fingerprint are modeled in a general dynamical system using ordinary differential equations with a parameter $\theta > 0$. | Studies need to be conducted more on arch structure from fingerprints. |
| 8 | MariiaNazarkevych et al.[8] | Multimodal biometrics is mainly used for certification and identity verification. Many biometric data are used for human authentication. | A better method than Ateb-Gabor Filters for Biometric Imaging can be made possible. |
| 9 | GianmarcoBaldini et al. [9] | Very high identification accuracy can be obtained in the electronic components using fingerprints. | Security threats could be present in the fingerprinting process itself. That means climate change affects the fingerprint image which may blur the image. |
| 10 | Young-Hoo Jo et al. [10] | Fingerprint verification is not only used to unlock these smartphones but is also used in financial applications such as online payment. | Fingerprints can be attacked by fake template synthesis using reverse-engineered rules and keys. |
| 11 | GianmarcoBaldini et al [11] | By taking advantage of defects and minute variances in the electrical components, which are referred to as "fingerprints" in this context, very high identification accuracy may be achieved. | Particularly for RF-based fingerprinting, the problem of fingerprint mobility is yet unresolved. |
| 12 | DindarMikaeel Ahmed et al [12] | Multiple biometric systems have more advantage than single biometric system. | The future of biometric trends is in the fields of medicine, finance, marketing, and many others where personal identification is required. |

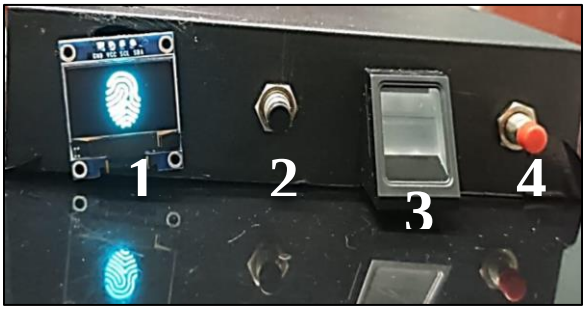


Figure 3: Fingerprint scanner with OLED display
Markings of the component:

1. OLED screen to show specific fingerprint information.
2. Increment button to increase fingerprint id while registering.
3. Fingerprint sensor to scan the finger.
4. The incremented value with fingerprint template is stored by holding the button.


Figure 4: Fingers with Different UID

User enters fingerprint id generated on the OLED screen as in Figure 5.

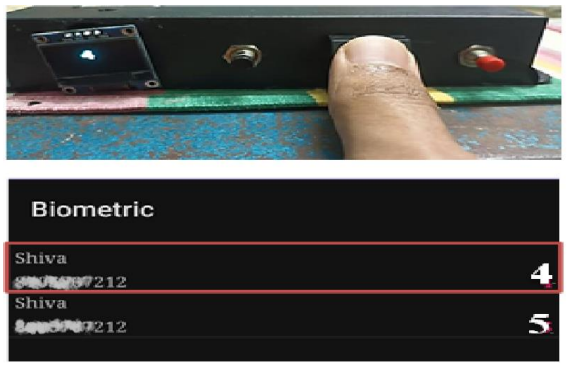


Figure 5: Fingerprint Registration Process

Users can register multiple fingers on same username to process SMF. Each fingerprint is stored on the database for the user-specified finger id. While authenticating an application, the user enters login credentials and the fingers to scan in the same order as it was registered. Each time the finger is scanned the sensor recognizes the fingerprint and displays the corresponding UID value on the OLED screen and matches it with the fingerprint id registered on the application. If the finger id is matched in sequence then the Login will be successful otherwise Login fails refer Algorithm shown in Table 2.

Table.2: Algorithm on SMF

**Input:** Accept Fingerprint Sequence
(For ex. 1+3+2+4+6 and each number recognizes individual fingerprints)

**Output:** return statement as Login Success or Login Failed

**1**: Convert numeric fingerprint sequence to string
(For the above ex. Converted string will be “13246”) store on database as Db_string

**2**: User logs in with uname and scan fingerprints with converted Pwd_string as password

**3**: if Db_string = = Pwd_string
**4**: then

**5**: return Login Success
**6**: else
**7**: return Login Failed

**8**: end if

The database stores login information of an application and fingerprint data. The user can register his name, mobile number, and fingerprint UID. For authentication, the user's ID and fingerprint ID are compared for validity and concatenated sequence as string. The user will be authenticated if both the strings are matched; else, the authentication fails as shown in Figure 6.

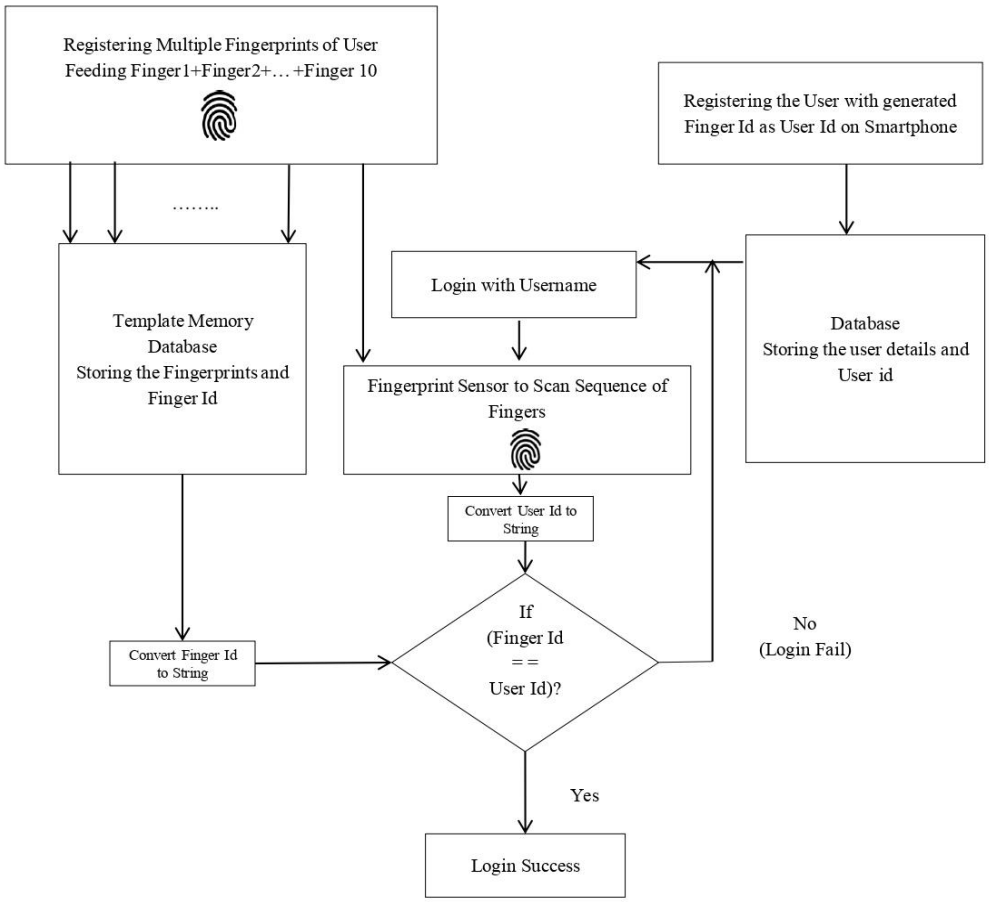


Figure 6: Flow Structure SMF

## 5. Experiment and Analysis

This section presents the experiments we have conducted on the simulation bed to authenticate smartphone with SMF. To understand the robustness of action we have made two sections each briefs us with its robustness and security on authentication.

i. Authentication performance

To evaluate the performance on sequence of fingerprint authentication, we calculate False Acceptance Rate (FAR) and False Rejection Rate (FRR). The FAR is calculated as the ratio of false acceptances with the total number of test samples considered as imposters; on the other hand FRR is calculated as ratio of false rejections of registered user with the total number of test samples [26] refer equations 1 and 2.

$$FAR = \frac{FA}{N} \quad (1)$$

$$FRR = \frac{FR}{N} \quad (2)$$

FA = False Acceptances
FR = False Rejections
N = Number of Test Samples

We have registered all the ten fingers of a user in a sequence by making a note of the readings of finger and its corresponding number as authenticated user and 10 individuals are considered as imposters who have not registered to the model. According to the experiment conducted we observed the authentication result shown in Table 3. At first the registered user placed all his ten fingers in sequence as registered earlier and the model showed login success by recognizing all his fingers and for the next

Table 3: Results Obtained on SMF

| | **Sequence of Fingers** | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Scans** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **FAR** | 0.2 | 0.1 | 0.1 | 0.3 | 0.3 | 0.2 | 0 | 0 | 0 | 0.1 |
| **FRR** | 0 | 0.1 | 0 | 0.2 | 0.2 | 0 | 0 | 0.3 | 0.2 | 0.1 |

authentication we made an imposter to scan his first finger and remaining 9 fingers was scanned by the registered user, the results are recorded in the Table 2 and the same way 10 different imposter samples are scanned for different fingers along with the registered user finger for other sequence scans. The result of FAR is shown in Table 3. In some test cases we got zero FAR value that means there is no false acceptance. The FRR is computed by repeating authentication process for 10 times by the authorized user, due to certain conditions such as wrong placement of the finger, moist finger or dry finger [10] [23] [22] we got few false rejection values as noted in table. For few fingers FRR value showed 0 that means there is no error in recognizing registered fingerprint.

The ROC curve (Receiver Operating Characteristic Curve) Figure 9(a and b) represents the working model on SMF with attributes True Positive Rate (TPR) and False Positive Rate (FPR) equation 3 and 4 obtained through the variables FAR and FRR that are computed on ratio of actual result divide by result obtained on the experiment we obtained from the Table 3. The ROC curves are categorized into two sections, the Figure 9a shows the ROC curve generated with involvement of imposter in each finger followed by registered user and the graph shows exponential growth of both FAR and FRR rates against actual and obtained threshold values. Figure 9b shows the same growth of FAR and FRR rates but without involving any imposters, the registered user scans the fingerprint in sequence for 10 different intervals and graph shown constant FAR after repeated scans and increase in FRR due to above mentioned conditions [10][23].

$$TPR = \frac{FAR}{P} \quad (3)$$

TPR = True Positive Rate
FAR = False Acceptance Rate
P = Number of Positive Outcomes

$$FPR = \frac{FRR}{N} \quad (4)$$

FPR = False Positive Rate
FRR = False Rejection Rate
N = Number of Negative Outcomes

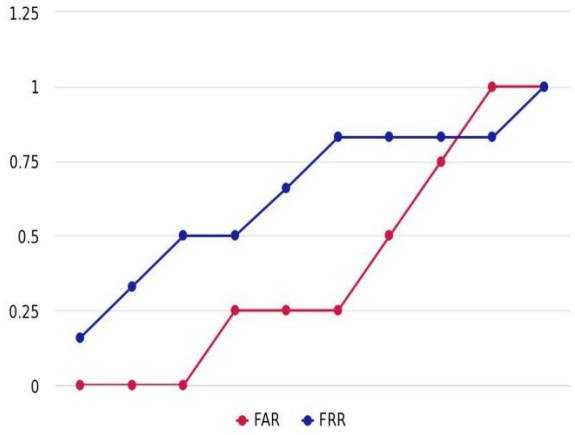


Figure 9 (a): ROC Curves with the Involvement of imposters on Sequence of Fingerprint Authentication

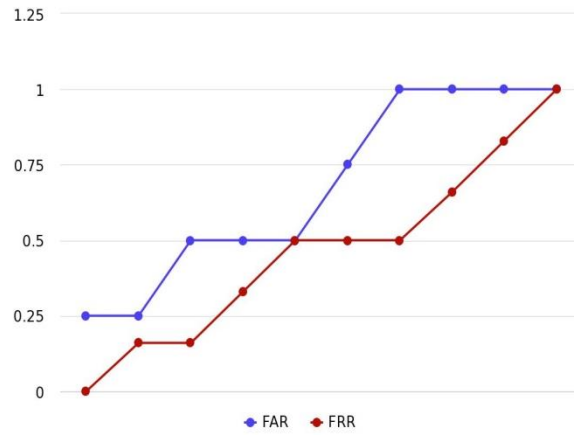


Figure 9 (b): ROC Curve Generated with Authorized User Authentication

ii. Stored Template Matching

The main fingerprint attack involves recovering the fingerprint feature points of the template after removing the stored template from non-volatile memory [10]. An attack known as "Attack on feature extractor module" can be made against the feature extractor module. The sensor provides the raw biometric data it receives when it sends raw data to the module extracting features. Instead of providing the feature values derived from the actual data acquired from the sensor, an imposter applies pressure to the feature extractor module to produce the feature values chosen by the imposter [24].

The impostor must change over the old template with the new one in order to attempt on modification. As explained in [10], the primary security problem in the current smartphone fingerprint system is that requirement for an imposter to replace a template for fingerprint scan and an imposter can replace single template [24] but replacing multiple templates becomes difficult task because of the combinations of the fingerprints assigned in sequence shown in Table 4, if we use the proposed technique on smartphones which increases the number of templates that need to be replaced. Hence this allows us to increase the robustness and security of smartphone. Combinations equation can be obtained to predict the number of fingers and templates.

$$nCr = \frac{n!}{(r!*(n-r)!)} \quad (5)$$

Here $n$ is number of fingerprints registered and $r$ will be number of fingerprint scanned at a time. The Figure.10 demonstrates the increased number of templates with the increase in registered fingerprints.

| Equation Substitution On ${}^{n}C_{r}$ | Templates Required to Replace |
|---|---|
| ${}^{1}C_{1}$ (min) | 1 Template |
| ${}^{10}C_{1}$ (max) | 10 Templates |

Table 4: Templates Required to Replace with Combinations

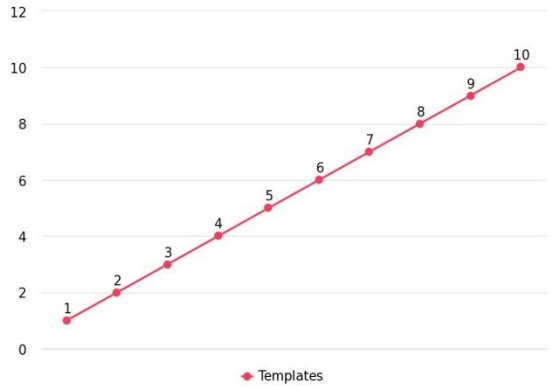


Figure 10: Demonstration of Increased Number of Templates Required Using SMF

From the above Figure.10, x-axis represents number of templates and y-axis represents number of fingerprint scans for the smartphone and by the combinations equation we compute that for 10 fingerprints, imposter requires 10 different templates for replacement that enhances the security and robustness of the system.

## 6. Results and Discussions

The results are divided based on the Accuracy, Security and Robustness, and Speed of the fingerprint sensor.

The softening filter is extensively used to remove noise in the picture in common and the form of a fingerprint in particular. It consists in scanning the whole image of the window N - dimensionality n*n and adapting the intensity value for each

pixel. The new value is calculated as the arithmetic mean of the value of all the pixels that fall into the window as shown in Equation 6.

$$I(i,j)=\frac{\sum_{(x,y)}^{N} I(x,y)}{n^2} \quad (6)$$

Here, I(i,j) is the new value of the pixel intensity with coordinates (i,j), and I(x, y ) is the initial intensity value for the pixel with coordinates (x,y). Likewise, the Median filter to remove the noise of pixels inside the piece window is sorted ascending (descending); the output value is the intensity of the pixel located in the middle of the list. The binary image is scanned by the n*n dimension window, for the mid pixel of the window with coordinates (i, j), and the reflection coefficient is calculated, which is equal to the ratio of the number of N(i, j) white pixels caught in the window to the dimension of the window as depicted in equation 7.

$$k(i,j)=\frac{N(i,j)}{n^2} \quad (7)$$

Here, k (i, j) - the reflection coefficient of the pixel with coordinates (i,j). Subsequently, a fresh intensity value for each pixel is calculated. The new value of the intensity of the pixel is equal to the product of the reflection coefficient on the maximum intensity of light as shown in Equation 8.

$$I(i,j) = k(i,j)\cdot I_{max} \quad (8)$$

Here, Imax is the upper limit of the value of intensity, I(i,j) - the value of the intensity of the pixel with coordinates (i,j). To normalize the image using the Gabor filter, needed to set the preceding mean values and deviations. A normalized image G is defined as an image where G(i,j)- is the value of the normalized brightness of the pixel with coordinates (i, j).

The normalized image is calculated based on the mean and root mean square deviation of the original image, where M and VAR - the output values of the mean and the mean square deviation, are calculated by the equations (9) (10):

$$M=\frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} I(i,j) \quad (9)$$

$$VAR=\frac{1}{N^2}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1}\left(I(i,j)-M\right)^2 \quad (10)$$

The orientation image is calculated from the normalized image. It is termed as an image where O(i,j) - the local orientation (angle of inclination) of the projection in the pixel with the coordinates (i,j) as shown in equation (11):

$$O(i,j)=\frac{1}{2}arctg\left(\frac{d_x^2(i,j)d_y^2(i,j)}{2d_x(i,j)d_y(i,j)}\right) \quad (11)$$

Here, dx( i, j) and dy( i, j) are the gradients of the pixel with the (i,j) coordinates on the axes X and Y respectively. Let Frequency Image F (i,j) be the local frequency of the protuberance, and let I - the number of pixels between two adjacent vertices of the crests in the dimension block W*W with the center of which is a pixel with coordinates (i,j), then the frequency in this pixel as shown in equation (12):

$$F(i,j)=\frac{1}{I} \quad (12)$$

The use of Gabor filters configured for the local orientation of the speeches applies to the normalized input image as shown in equation (13):

$$G(x,y)=exp\left(-\frac{1}{2}\left(\frac{x_\varphi^2}{\sigma_x^2}+\frac{y_\varphi^2}{\sigma_y^2}\right)\right)cos\left(2\pi\theta x_\varphi\right) \quad (13)$$

Here,$x_\varphi = xcos(\varphi) + ysin(\varphi)$; $y_\varphi = -xsin(\varphi) + ycos(\varphi)$; $\varphi -$ is the orientation of the Gabor filter, $\theta$- the frequency of the sinusoidal plane wave, and $\sigma_x^2$ and $\sigma_y^2$ is the space constants of the Gaussian bypass along the axes x and y, respectively. These constants are established and adjusted based on empirical data on the operation of the algorithm.

i. Finding the accuracy of fingerprints

Based on the analysis of several papers it is clear that fingerprints cannot be 100% accurate

because of external factors like image quality and matching algorithm. The accuracy of a fingerprint can be evaluated by using the performance indicators e.g., False Accept Rate (FAR), False Reject Rate (FRR), and Equal Error Rate (EER) [23] [22].

To calculate the accuracy of the single fingerprint we can evaluate the equation 14:

$$ACR = \frac{\text{FAR+FRR}}{2} \quad (14)$$

ACR=Accuracy of the Fingerprint Sensor

Most biometric scanners show an accuracy of detecting the fingerprint of more than 90% [16]. In the experiment conducted by SAGEM of France and Cogent, an American company, according to them, the most accurate system was NEC of Japan which showed 98.6% accuracy for the single finger test [16]. Based on the above data the accuracy for the sequence of multiple fingerprints for 10 fingers can be achieved using equation 15:

$$\text{ACS} = \sum_{ACR=1}^{10}(\text{ACR})/10 \quad (15)$$

ACS=Accuracy of Sequence Fingerprints

As a result, there is no change in the accuracy when the sequence of multiple fingerprints is implemented.

ii. Finding the Security and Robustness of Fingerprints

The security and robustness can be evaluated using the performance indicators such as Spoof Acceptance Rate (SAR) and Imposter Acceptance Rate (IAR). To calculate the Security and Robustness of the single fingerprint below equation 16 can be evaluated:

$$\text{SAR} = \frac{\sum_{k=1}^{E} \text{S}_i}{(UXE)} X100 \quad (16)$$

From the above equation,

E- Number of Enrollments

U- Number of Unlock Attempts

Si- Number of Successful Unlocks

To calculate the Security and Robustness of the Sequence of 10 fingerprints same equation need to be enhanced by making it more complex by substituting the equation 17 with summation 10 times:

$$SAR = \sum_{n=1}^{10}\left[\frac{\sum_{k=1}^{E} \text{S}_i}{(UXE)} X100\right] \quad (17)$$

From the above equation,

E- Number of Enrollments

U- Number of Unlock Attempts

Si- Number of Successful Unlocks

n- Number of Fingerprints

As we increase the number of fingerprints to authenticate the security and robustness increase with the increase in complexity.

iii. Finding the Speed of multiple fingerprints

For the ultrasonic sensor, once the fingerprint is registered, it will deliver an unlocking speed of 0.2 seconds. To evaluate the speed of the sequence of fingerprints we can use the equation 18:

$$Speed = \sum_{n=1}^{10}[x] \quad (18)$$

Where x is the present fingerprint recognition speed i.e. x=0.2. If we try to equate the value x for 10 sequence fingers then the combined result would be 2 seconds. Even though the speed of fingerprint recognition is delayed 10 times more we can predict that the accuracy, security, and robustness have been increased thus enhancing the present security.

iv. Performance of multiple fingerprints

In the multiple fingerprint assessments, simulation was used to integrate the software of the fingerprint profiles configured on Hardware and Android Smartphones, compared comprehensively on various runs using different fingerprints, and tried obtaining two (R1, R2) samples with evaluation results as shown in Figure.11.

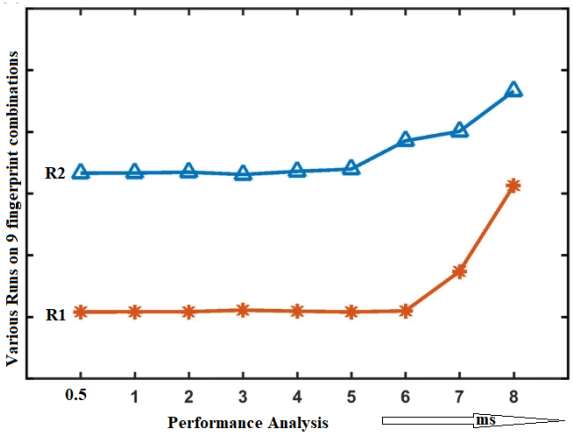


Figure.11. Performance Evaluation

To demonstrate the success rate of both single and sequence of multiple fingerprints we have used a graph where the x-axis represents the number of authentication attempts and the y-axis represents

the success rate shown in Figure 12. In single Fingerprint, the success rate initially rises rapidly as the number of authentication attempts increases, signifying successful authentication with a single fingerprint. However, the graph can reach its maximum at some peak point and then shows constant or plateau rates, as seen in the graph, or it might begin to decline due to the increase in the false acceptance rate [12]. The single fingerprint shows a high FAR rate. Although the success rate of multiple fingerprint authentications may start at a lower rate than that of single fingerprint authentication, as you can see in the graph, there will not be any decline in the success rate as the number of authentication attempts increases.

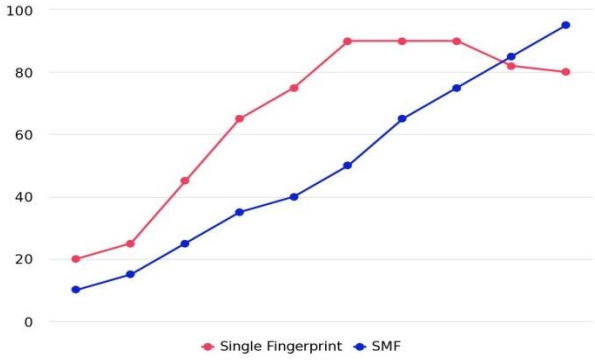


Figure.12. Success rate Comparison

## 7. CONCLUSION

The smartphone uses fingerprint techniques for authentication for several applications including phone unlocking so the imposter may try to access the fingerprint of a registered user if the number of fingerprints is limited to one as in existing smartphones then security and robustness will be very low, it is very much essential to enhance authentication process. The existing authentication methods can be improved through SMF technique. This paper provides an idea of SMF technique and describes the design details of how we can overcome the problem of single fingerprint authentication by implementing the proposed methodology. We have compared the results of single fingerprint and SMF authentication; it is observed that the success rate of SMF increases without declining on several authentication attempts. Experimental analysis shows that FAR achieves minimum rates as the authentication attempts increase such as 0.2, 0.1, 0.1, 0.3, 0.3, 0.2, 0, 0, 0, 0.1. Stored templates and other fingerprint-accessing attacks can be reduced through SMF technique as it provides robustness to the system. FRR rates are also computed and analyzed for the registered user.

The results are discussed by comparing SMF with a Single fingerprint upon several techniques. Enhanced equations are derived based on the Accuracy, Security and Robustness and Speed of the fingerprint sensor and it is observed that accuracy remains the same after applying SMF technique and robustness provides better complexity compared to single fingerprint authentication and the speed of the authentication process increases with the increase in fingerprint sequence. The main problem with SMF technique is that it is time-consuming for the user while registering the fingerprints. Once the fingerprints are registered in sequence user needs to remember the specific sequence. So this work needs further research to simplify the process of authentication without affecting security and robustness. However, there are still unaddressed problems regarding how to further increase the practical security and robustness of this technique, which will be covered in the future.

## REFERENCES:

1. Jung, Hanyung, SoobinSim, and Hyunkoo Lee. (2023). Biometric authentication security enhancement under quantum dot light-emitting diode display via fingerprint imaging and temperature sensing. *Scientific Reports 13.1,2023,794*.
2. Chen, Yu, Yang Yu, and Lidong Zhai. InfinityGauntlet: Brute-force Attack on Smartphone Fingerprint Authentication.
3. Martin-Escalona, Israel, and Enrica Zola. (2023). Improving Fingerprint-Based Positioning by Using IEEE 802.11 mc FTM/RTT Observables. *Sensors 23.1, 2023,267*.
4. Abdullah Saud., NazarElfadil. (2020). Biometric Authentication by Using Fingerprint Recognition System.

5. Sabt, Mohamed, Mohammed Achemlal, and AbdelmadjidBouabdallah. (2015). Trusted execution environment: what it is, and what it is not. *IEEE Trustcom/BigDataSE/Ispa. Vol. 1. IEEE*.
6. JieChang., XiaojunZuo., BotaoHou., Shuo Liu. (2021). Mobile APP fingerprint feature. 2021 extraction pattern recognition based on Random Game.
7. Busch, Marcel, Johannes Westphal, and Tilo Müller. (2020). Unearthing the TrustedCore: A Critical Review on Huawei's Trusted Execution Environment. *WOOT@ USENIX Security Symposium*.
8. Jawarneh, Ibrahim, and NesreenAlsharman. (2020). A mathematical model for arch fingerprint. *arXiv preprint arXiv: 2003.00308.*
9. MariiaNazarkevych, Natalia Kryvinska., YaroslavVoznyi. (2021). Applying Ateb–Gabor Filters to Biometric Imaging Problems.
10. Young-HooJo., Seong-Yun Jeon., Jong-HyukIm., Mun-Kyu Lee. (2016). Security Analysis and Improvement of Fingerprint Authentication for Smartphones.
11. GianmarcoBaldini, *member, IEEE* and Gary steri. (2017). A Survey of Techniques for the Identification of Mobile Phones Using the Physical Fingerprints of the Built-In Components.
12. DindarMikaeel Ahmed.,Siddeeq Y. Ameen., Naaman Omar.,Shakir Fattah Kak.; ZryanNajat Rashid.,HajarMaseehYasin.,IbrahimMahmood Ibrahim.,AzarAbidSalih.; Nareen O. M.Salim .,Awder Mohammed Ahmed. (2021). A State of Art for Survey of Combined Iris and Fingerprint Recognition Systems.
13. EmanueleMaiorana.,HimankaKalita.,PatrizioCampisi. (2020). Mobile keystroke dynamics for biometric recognition: An overview.
14. JannisPriesnitz., Rolf Huesmann., Christian Rathgeb., Nicolas Buchmann., Christoph Busch. (2021). Mobile Touchless Fingerprint Recognition: Implementation, Performance and Usability Aspects.
15. Maryah E. M. Haertel.,Eduardo J. Linhares.,André L. de Melo. (2020). Smartphones for latent fingerprint processing and photography: A revolution in forensic science.
16. Peng, Chang. (2020). Thin-film-based transducer for under-display ultrasonic fingerprint sensing applications. *IEEE Sensors Journal 20.19.*
17. 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.*
18. Hemalatha, S. (2020). A systematic review on Fingerprint based Biometric Authentication System. *International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE). IEEE.*
19. Sengar, Sandeep Singh, U. Hariharan, and K. Rajkumar. (2020). Multimodal biometric authentication system using deep learning method.*International Conference on Emerging Smart Computing and Informatics (ESCI). IEEE*.
20. Zukarnain, Zuriati Ahmad, Amgad Muneer, and Mohd Khairulanuar Ab Aziz. (2022). Authentication securing methods for mobile identity: Issues, solutions and challenges. *Symmetry 14.4 (2022): 821*.
21. Chen, Yu, and Yiling He. (2023) BRUTEPRINT: Expose Smartphone Fingerprint Authentication to Brute-force Attack. *arXiv preprint arXiv:2305.10791 (2023).*
22. Shen, Chao, et al. (2017). Performance analysis of multi-motion sensor behavior for active smartphone authentication. *IEEE Transactions on Information Forensics and Security 13.1 (2017).* 48-62.
23. Jain, Rubal, and Chander Kant. (2015). Attacks on biometric systems: an overview. *International Journal of Advances in Scientific Research* 1.07 (2015): 283-288.
24. Eric Setterberg. (2020). Before the ink is dry: Correcting biometric spoofing myths.
25. Huawei. Security advisory - fingerprint unlocking vulnerability on smartphones, (2018). https://www.huawei.com/br/psirt/ security-advisories/2018/huawei-sa-20180203-01-fingerprint-en.
26. Industries, Adafruit. Fingerprint Sensor. Fingerprint Sensor : ID 751 : Adafruit Industries, Unique & Fun DIY Electronics, and Kits, www.adafruit.com/product/751.

27. Introduction to Nodemcu: Nodemcu. *ElectronicWings*, www.electronicwings.com/nodemcu/introduction-to-nodemcu. Accessed 9 June 2023.
28. What Is an OLED? *Ossila*, www.ossila.com/en-in/pages/what-is-an-oled.
29. Measuring Biometric Unlock Security | Android Open Source Project. Android Open Source Project, source.android.com/docs/security/features/biometric/measure.