I.J. Information Technology and Computer Science, **2022, 4, 34-47**
Published Online August 2022 in MECS (http://www.mecs-press.org/)
DOI:10.5815/ijitcs.2022.04.04

Smartphone-based Biometric Authentication Scheme for Access Control Management in Client-server Environment

Sajaad Ahmed Lone
Department of Electronics and Communications Engineering, National Institute of Technology Srinagar, Jammu and Kashmir, India
E-mail: sajaadlone@iust.ac.in

A.H. Mir
Department of Electronics and Communications Engineering, National Institute of Technology Srinagar, Jammu and Kashmir, India
E-mail: ahmir@rediffmail.com

Received: 10 January 2022; Revised: 06 March 2022; Accepted: 23 March 2022; Published: 08 August 2022

Abstract: As the information put together by the blend of smartphones, the cloud, the IOT, and ubiquitous computing continue to expand at an alarming rate, a data breach increases. Today, users' strong authentication and authorization approaches are increasingly important to secure sensitive, confidential, secret information. Possession and knowledge-based authentication techniques for computers, the internet, email accounts, etc., are commonly used to access vital information; they do not link a user to an established identity, resulting in most security vulnerabilities. Biometric authentication, on the other hand, has the privilege of being more reliable than traditional authentication as biometric characteristics of a person can't be lost; they are tough to distribute, exchange or duplicate; and it requires the user to be present during the authentication process, thereby relating the users to established identities. Biometrics provides a higher level of assurance that the individual attempting to ascertain is the individual in question. Thus, resulting in a more reliable, usable, and cost-effective model with a higher level of protection to deter an attacker from obtaining entry to a computer or network and gaining access to confidential data. This paper introduces a novel fingerprint-based authentication scheme for mobile environments, enabling user authentication based on fingerprint features using a challenge-response-based authentication process. In this study, the proposed authentication system has been developed on a real Android-based smartphone, tested on actual users, and performance analysis has been carried out; empirical results reveal that the proposed authentication scheme achieves increased performance. Moreover, a usability analysis has been done to determine efficiency, effectiveness, and user satisfaction. The evaluation results indicate its feasibility to use it as an effective authentication mechanism for mobile phone environments.

Index Terms: Biometrics, Fingerprint, Authentication, Challenge-Response, Smartphone.

1. Introduction

The wonders of technology have changed every aspect of our lives, and the enormous impact has been that of the smartphone. Smartphones in the current era enable consumers worldwide to communicate more effectively, pay online bills, shop, and even remotely control devices in their homes and cars[1]. Over time, mobile devices have come to deliver many high-quality novel features in processing power, storage, and state-of-the-art sensors, which has increased customers' interest. Most organizations in today's world take advantage of smartphone devices' ubiquity and create their applications to enable their clients to conduct transactions while on the move[2]. Because of the growing popularity of these mobile applications for accessing e-commerce and other business services, security and privacy have become major concerns[3]. Performing safe transactions and accessing sensitive data necessitates security measures that provide reasonable protection against imminent threats. Security measures based on knowledge for access control across digital networks are still used in security modernization in the current era because they are cost-effective to install and easy to revoke in the event of a breach[4]. The primary issue with these systems is that they do not identify individuals with established identities and thus do not authenticate the person who has been enrolled. Accordingly, the most reach of personal information appear to result from poorly and compromised passwords being recalled; in most cases, the users themselves have no apparent memory of their passwords and cannot resist using easy-to-to-remember passwords. Stolen and reused passwords make data useless when critical data is exposed further. In a nutshell, knowledge-based

authentication such as password schemes appears to have no role in the world of mobile payments, where financial and identity theft is high. Various schemes are implemented to replace complex passwords with token-based authentication approaches such as smart cards, hardware keys, and chip modules. They provide a more robust protection but lack user-friendliness, are unreliable, can be lost, duplicated, or stolen, and are expensive and unwieldy, restricting their usage[5–7]. To circumvent the constraints of the authentication mechanisms based on knowledge and possession, an alternate method that is quick and secure is necessary for user authentication in mobile environments. Integration of various capturing devices such as cameras, microphones, touch screens, and swipe sensors for a fingerprint in mobile phones encourages developers to devise alternative authentication solutions based on biometrics. Authentication schemes based on biometrics are more secure than traditional passwords, as in these schemes, individuals' physical and behavioral characteristics are used for authentication. These authentication schemes provide a higher level of certainty about the legitimate user and make it near-impossible to deceive the authentication system; thus, it could be an alternative authentication scheme to access sensitive and critical information using mobile phones. As mobile devices are personal and usually dedicated to an individual, biometrics is an obvious choice for study and implementation[8–11]. In light of the benefits of biometric authentication, in the present study, a biometric-based authentication technique is especially suited for mobile devices has been developed that can be utilized in client-server contexts and a hybrid environment. With the proposed authentication strategy, the fundamental concept is to develop an authentication mechanism that employs biometric (fingerprint) features as a secret key between the client and the server to generate a one-time password for each client and server transaction. The current scheme makes use of application-based authentication, which ensures data confidentiality and improved security. For example, in the challenge response authentication mechanism, the server sends a different challenge value to the client each time, resulting in the generation of a one-time password. Thus, making it more secure and user-friendly when authenticating genuine users in mobile applications that are used to access crucial information. Moreover, the performance and usability analysis of the proposed authentication technique proves that the proposed authentication is effective, efficient and user-friendly for mobile phones environments.

As for the rest of this work, it is organized as follows. Section 2 provides background information on automatic biometric authentication systems and fingerprint authentication as authentication techniques in smartphone contexts. Section 3 describes the proposed fingerprint-based authentication mechanism that we have developed. Section 4 presents the experimental findings, performance and usability evaluation of the scheme proposed, and Section 5 summarizes the conclusions drawn from the results. In Section V, we give a brief review of the contributions that have been made and some suggestions for future work.

2. Background and Related Work

The widespread availability of powerful computing devices such as smartphones, tablets, and laptops has changed the way people interact with various online services provided by banks, health care and other industries. The expanding use and reliance on these gadgets also suggest increasingly processing and storing private and sensitive information. The risk and cost of losing sensitive data increase as more sensitive data is kept in or accessible through mobile devices. As a result, mobile devices should include very high-security features for personal information and privacy protection through individual identity against unauthorized usage in the event of theft or fraud. In any computing system, the user authentication process is the first line of protection that verifies that the user is who they claim to be. Today, three universally acknowledged authentication factors based on knowledge, possession, and biometrics are used to authenticate legitimate users[12–18]. Authentication based on knowledge and possession has a specific limitation that makes them susceptible to various attacks. With the recent advancements in smartphone and wearable mobile digital technologies, biometrics are becoming increasingly mainstream[3, 4, 19–24]. Not only have existing mobile companies incorporated biometric capturing sensors, but the new potential of these authentication mechanisms has also attracted the curiosity of law enforcement agencies and the banking sector[25]. In light of these advancements, many principles involved in developing biometric authentication in mobile environments are critically examined in this section.

2.1. Biometric Authentication Systems

In computing, biometrics refers to a system that recognizes or identifies people based on their own patterns of physiological or behavioral characteristics. Without any authority or knowledge, a person's identity could be determined using biometrics and are valued for their uniqueness and stability, making them a suitable biometric identifier[15, 24, 26–32]. Biometric characteristics cannot be lost or overlooked, they are challenging to replicate, distribute or trade, and they require the user to be lively at the point of authentication; they are perfectly secure than other forms of authentication. Over several decades, researchers have put many efforts into developing automatic biometric authentication systems, which dramatically reduced the identification and verification processes[33–35]. A biometric authentication system is a computerized technology that collects, processes, and stores information about an individual's biometric features to determine that individual's identity[33-34]. With the introduction of more powerful computers, identifying biometric records within a database of millions of records has also become much faster. Generally, a biometric authentication system comprises of four modules as shown in fig.1. A sensor module: a biometric trait that

has to be identified is sensed, a feature extraction module: from the perceived image, a machine representation (pattern) is extracted, a template database, and an identification matching module: representations deduced from the perceived image are compared to a system-stored representation, all of which are interconnected [36–44].

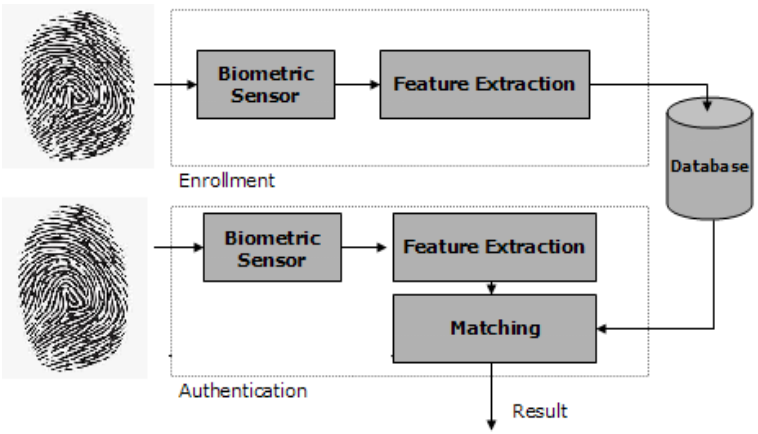

Fig.1. General Architecture of Biometric Authentication System

Fig.1 illustrates how a conventional biometric authentication system authenticates users during enrolment and verification stages. The sensor scans the user's biometrics to get a digital image in the enrollment mode. The features are extracted from the sensor's image acquired and transformed to provide template data for comparison during the verification stage. During the verification mode, the sensor module also takes an image of the query. The feature representations of the query biometric image are treated to the same technique as they were during the enrollment step to receive query data. Afterwards, the query information is compared with the template to arrive at a matched result[43–47]. Many security studies are based on biometrics covering both a person's physiological and behavioral traits. The following are some biometric-based security systems that have been revived for the current study.

A. Physiological Characteristics Based Authentication

Biometric authentication techniques based on physical features or characteristics of a person form the basis of physiological-based authentication schemes. The physical attributes of the face, retina, iris, palm, hand geometry and fingerprint are among those that have remained generally unaltered over time.

a. Fingerprint recognition

Fingerprint-based authentication is a popular study topic in mobile environments for authentication. These authentication techniques have already been deployed on mobile phones and can be viewed as a user-acceptable approach for determining an individual's identification. It has been proposed in [48] a fingerprint-based authentication technique, developed as an Android application and operating on actual smartphones. A total of three authentication methods for fingerprint recognition have been presented, each of which assessed based on its accuracy and speed of processing, respectively. In contrast, [49] proposes a reliable, low-cost, and stable fingerprint authentication technique for mobile phone devices that are both simple and effective. The system was developed with the help of the OpenCV (Computer Vision) library and the Android operating system. The RGB matching method has been employed in this instance. These fingerprint-based authentication techniques look inexpensive and straightforward, and they do not appear to consume a lot of battery life on resource-constrained mobile phones. However, due to the lack of hardware on mobile devices that are capable of obtaining the whole fingerprint, as well as incompatibility of fingerprint recognition methodologies in the presence of dirt or cuts, fingerprint-based security solutions appear to be some weaknesses in the field of developing a secure and available for adoption user solution for the masses.

b. Face recognition

When it comes to face-recognizing authentication techniques, they involve using facial features collected from digital images or video frames to verify or identify a particular individual. Face recognition is also a viable research topic in mobile authentication, and it has the potential to be very useful. The authors of [50] have developed a highly effective open face recognition-based authentication system for the Android system. The proposed system implements face, eye detection, LBP (Local Binary Pattern) for feature extraction, pre-processing for Region of Interest (ROI), feature dimensionality reduction based on Linear Discriminant Analysis (LDA) referred to as Fisherface and Principal Component Analysis (PCA) referred to as Eigenface, and Euclidean distance as a minimum distance classifier the experiments, the Fisherface algorithm was shown to be 96.0 per cent accurate in face recognition, and the Eigenface method was found to be 93.8 per cent accurate in face recognition. The face is the essential biometric attribute when designing mobile phone equipment compared to fingerprint and iris[51, 52]. However, even if mobile phone users

generally accept the authentication technique, there are still issues with the security solution's performance under certain conditions such as different facial angles, low lighting conditions, and various expressions that must be considered.

B. Behavioral Characteristics based on authentication.

It is possible to identify persons through behavioral biometric authentication, which comprises their specific activity or manner, such as voice, keystroke dynamic, and touch dynamic.

a. Behavior Profiling

Individuals' interactions with the mobile phone to make use of a wide range of services provide the basis for identifying an individual in such approaches; instances of such type include application usage, location, and other factors. For example, in [53], behavioral biometrics information was collected and analyzed from various Android mobile devices to give a solution for active authentication, which is intended to verify the identification of a genuine user continuously. Four biometric parameters: i) text entered through a soft keyboard, ii) device's physical location as per GPS (outdoors) or Wi-Fi (indoors) iii) used applications, iv) visited websites have been considered. A classifier has been developed and evaluated for each modality, and these classifiers are organized into a parallel binary-decision fusion design. Further, In [54], a novel access control system based on a specific user context has been implemented, dynamically giving or revoking user privileges based on the user's context. The authors have developed the strategies for Android restriction. Various closely neighbouring sub-areas within the same location can be distinguished by the context implementation, which is capable of distinguishing between them. While the setting in this paper has been determined by reference to time and location, the latter has been defined by reference to the presence of visible Wi-Fi access points and the strength of their signals and the use of cellular triangulation and GPS when these technologies are available. Despite this, such security measures are achievable on mobile phone devices. Performance inconsistency caused by unanticipated involvement by users, on the other hand, is the most significant issue that such systems have encountered so far.

b. Keystroke Dynamics

In this technique, a person's typing rhythm and style are considered. In smartphones, keystroke dynamics have been around for a very long time. In [55], the author aims to improve the existing systems based on keystroke dynamics authentication to increase the security of smartphones by improving user comfortability, such as the ability to change the PIN without any need Keystroke-Dynamics-Based-Authentication (KDA) system to be retrained. In comparison to physiological authentication-based techniques, this is a more comprehensive approach to achieving transparent active authentication without additional hardware; behavioural biometrics are being used more frequently. This results in an overall less expensive option than physiological authentication techniques. According to the survey results, physiological authentication techniques appear to be susceptible to replay attacks, in which an intruder can exploit the images of the physical traits by repeating them afterwards.

Furthermore, there is a strong incentive to increase security in the case of behavioural authentication techniques. Several ways can be used to counteract such susceptibilities while also increasing security. The author in [56] presented a framework that integrates the permuted sequence that constitutes behavioural fingerprint with the physiological fingerprint to bring together the reliability and accuracy of the two methods. If a user's fingerprint is compromised, the behavioural fingerprint works as a firewall, delaying or blocking unauthorized access to the system. The proposed behavioural fingerprint framework can identify the origin of a fingerprint and the sequence of fingerprints. It is more effective than multimodal biometric techniques and does not necessitate the purchase of any additional hardware.

Further, in [57], a biometric multimodal system for access control is described, which uses biometric traits such as the iris, the face, and the periocular to identify users. It has been demonstrated that multimodal fusion may be conducted using iris and face and periocular data. A weighted fusion strategy has been used to combine the comparison score of separate feature extraction schemes. This method investigates multiple score-level fusions to make use of the complementing information from the three modalities more efficient.

2.2. Fingerprint as an Authentication Technique in Smartphones

As more internet services are accessible through mobile phones resulted in a growing number of sophisticated cyberattacks, forcing businesses to innovate and develop newer methods of protecting the devices and accounts of the users from being compromised. The availability of a wide variety of sensors and other dynamic and user-specific information can strengthen user authentication using mobile devices[58–61]. Authentication based on knowledge is commonly used to access critical and sensitive information through mobile phones; although widely used in several modern applications, it cannot meet stringent security performance requirements. Most recent average mobile phone models have built-in biometric capturing features primarily for face, fingerprint and other biometric traits, which can be utilized to construct biometric security systems as a potential substitute to knowledge-based authentication systems such as passwords and PINs. When it comes to biometric authentication methods on smartphones, tablets, and laptops, fingerprint, iris, face, and voice recognition technologies are most commonly used. Among all biometric authentication methods, fingerprint recognition has the highest acceptability for identifying an individuals' identity due to its

popularity because of historical considerations and high recognition accuracy, permanence, and collectability[59, 61–67]. According to the International Federation of Biometrics, because of the rising use of fingerprint reader technology by numerous smartphone manufacturers, fingerprint reader technology has gained a substantial market share; the share is expected to reach $52.61 billion by 2022. Using fingerprints for authentication has several advantages, the most important of which is that they are uniquely linked to the individual, making fingerprints to mitigate the security and usability concerns associated with traditional knowledge-based solutions[15], [58, 68, 69]. As stated by the leading mobile fingerprint technology manufacturer Apple, the possibilities of different misclassifying fingerprints are just 1 in 50,000, but guessing a four-digit password is 1 in 10,000. Privacy concerns are alleviated using fingerprints for identification by only storing a mathematical representation of the fingerprint rather than the actual image. These advantages explain why fingerprint recognition is considered more reliable than other knowledge-based solutions by 90 percent of current users. Compared to password-based authentication systems, an attacker's significant complications in copying a user's fingerprint are serious. An individual's fingerprint cannot be changed: once a fingerprint has been declared invalid, it can no longer be used as a method of identification by the user. Unlike text passwords, fingerprints do not give the same amount of flexibility as text passwords, which may be changed by simply asking the person who created the fingerprint to alter their password[70, 71]. Function creep, which uses the same fingerprints for multiple systems to authenticate them, increases identity theft risk. Other factors such as skin, sensor conditions, injuries, and wet fingers could complicate the authentication process in mobile phone environments by increasing fingerprint images' pre-processing and resources[72–74].

3. Design of Proposed Fingerprint-based Authentication Scheme

Security in user authentication is becoming a significant apprehension in modern society since it is critical to confirm its identity in many consumer applications, particularly financial transactions, to ensure its security. A biometric authentication approach based on physical and behavioral characteristics has been offered in this circumstance as an alternative to traditional systems that depend on basic passwords, PINs, or tokens. Despite its multiple benefits, there are various unresolved challenges related to biometric authentication. Consequently, it is anticipated that a suitable authentication process that is secure, efficient, cost-effective, easy to use, and that can be implemented without incurring substantial changes in current infrastructure would be designed and deployed. This study intends to build an authentication system based on biometrics that authenticates individuals more user-friendly manner by using Android-based smartphones to access vital services via the internet that require robust authentication mechanisms in a client-server ecosystem. The fundamental concept of the proposed biometric-based authentication scheme is to design and develop a challenge-response identification or authentication method based on fingerprint characteristics where the fingerprint is being shared as a secret key within the client and server prior to authentication. The proposed authentication strategy uses application-based authentication, ensuring data secrecy while also providing increased safety, security, and user-friendliness. As with the challenge-response process n system, the server delivers a challenge value to the client each time in a different way, resulting in a one-time password for every session. The proposed fingerprint-based authentication scheme comprises two processes: fingerprint registration and fingerprint verification. The complete process of the proposed scheme is shown in Fig 2.

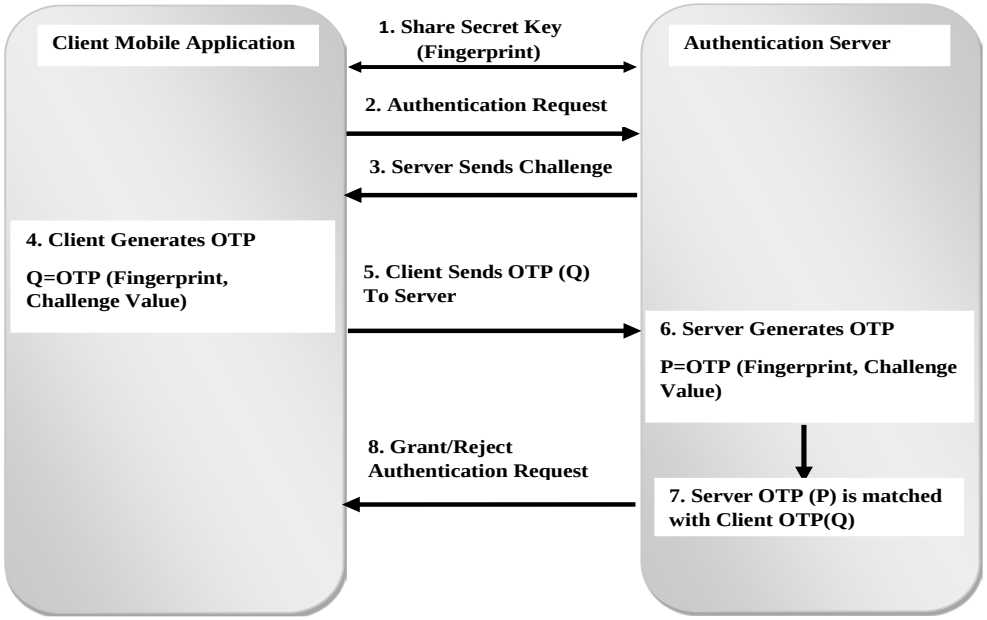

Fig.2. Proposed Fingerprint Based Authentication Scheme

During the registration process, the user's fingerprint is captured using a smartphone application, and the feature extractor module extracts features based on minutiae and stores them in the database on the server; these fingerprint features are shared between client and server as a secret key. When the server verifies the client's identity via the verification process, a challenge value is sent to the client to complete the verification. The user scans fingerprint already registered; the client generates an OTP based on fingerprint and challenge value and sends it to the server. Complete fingerprint feature extraction and OTP generation process are explained in 3.1. The server generates an OTP value based on a previously registered user fingerprint in the database by employing the same process as the client. The OTP value generated by the server is matched to the one sent by the client; if they match, the legitimacy of the user is deemed authentic; if they don't, the user isn't.

3.1. Fingerprint Feature Extraction and One-time Password Generation Process

As a biometric trait, fingerprints are the most widely known for more than a decade, the technology has been used to identify criminals and solve crimes, and because of its accuracy and secrecy, it continues to be a significant instrument for law enforcement. Fingerprint recognition has become more prominent as fingerprint scanning technologies are integrated into smartphones, computing devices, and tablets, making it easier for users to authenticate and access key services. If we compare fingerprint-based identification systems to other biometric features, they have undergone extensive testing, with no examples of attempts to defraud the system so far. Several studies have found that the fingerprint-based authentication approach has a high level of accuracy. While certain factors like dust, cosmetics, and aging might result in false positives and negatives, the fingerprint feature has been shown to have an error rate of 1 in 500 or more, making it more accurate than other biometric traits[75–79].

A fingerprint is a distinctive pattern produced by friction ridges (raised) and furrows (recessed) on the pads of the fingers and thumbs that are unique to the person. On the finger, the ridge is a raised section of the epidermis that remains in place throughout a person's life. A valley is defined as the area between two ridges that meet head-to-head. Ridges and valleys can occasionally be found going parallel to each other, bifurcating and terminating at different spots along the way. Fingerprints can be classified into the following basic categories, as illustrated in Fig. 3, based on ridge creation in the fingerprint [80].

Fig.3. Fingerprint Patterns

Identifying the most apparent structural characteristics on the fingerprint surface known as minutia, which is essential to distinguish among fingerprints, is not a difficult task to detect. Among almost 150 diverse forms of minutia, ridge termination and ridge bifurcation are the most often used for identification. It is possible to see the remaining of minutia as a blend of these two. The core and delta points, both of which are commonly referred to as unique points, are two critical locations for fingerprints. It is common for them to be defined by areas of substantial curvature when the ridge abruptly changes, and they are used to categorize images of fingerprints to narrow the search space available for analysis. These points are the most important fingerprint traits since they are exceedingly stable and scale and rotation-invariant when viewed at a high level. Fingerprints with singular points, such as cores, are most accurate and reliable, and they may be detected in most cases. It is the region in the fingerprint ridge with the greatest curvature and the highest point among the inner ridgelines inside the fingerprint. As defined in a fingerprint, the core point is a precise position that can be used as the starting point for determining other minutia points in later calculations [78, 81–83]. It is possible to distinguish between fingerprints occupying the same relative area and location by perceiving and comparing their minutia characteristics. An orientation field image is used to find singular points in this study, and different strategies are proposed. The Poincare Index Method is adopted in the current analysis, which is a widely used and practical way for detecting these points from a fingerprint[81, 82, 84–86]. To apply the Poincare Index Method to fingerprint source images, it first needs to be translated into an orientation field, which can then be applied. The Poincare index of all the points is calculated by totaling up the field angle differences of consecutive points in the orientation image, with the highest Poincare Index being the point contained by a digital curve (Core Point). We consider the following scenario: eight locations are taken in the neighbourhood of a specific target point. For a position (i, j), let (i_0, j_0) = (i, j + 1), (i1, j1) = (i + 1, j + 1), (i2, j2) = (i + 1, j), (i3, j3) = (i + 1, j−1), (i4, j4) = (i, j−1), (i5, j5) = (i−1, j−1), (i6, j6) = (i−1, j), and (i7, j7) = (i−1, j+1).

Let θ (i, j) be the (i, j)-element of an orientation field image and $0 \leq \theta (i, j) < 2\pi$ for any (i,j)

$$\text{Let } \delta k(i,j) = \theta (ik+1, jk+1) - \theta (ik, jk) \quad (1)$$

for $0 \leq k \leq 6$ and $\delta 7 = \theta (i_0, j_0) - \theta (i_7, j_7)$. Then the Poincare Index of an element (i,j) is defined to be

$$P(i,j) = 1/2\pi \sum_{k=0}^{7} \Delta_k(\mathbf{i},\mathbf{j}) \quad (2)$$

Where

$$\Delta k(i,j) = \begin{cases} \delta_k(i,j) & \text{if } |\delta_k(i,j)| < \pi/2 \\ \pi + \delta_k(i,j) & \text{if } \delta_k(i,j) \leq -\pi/2 \\ \pi - \delta_k(i,j) & \text{otherwise} \end{cases} \quad (3)$$

The value of the Poincare Index is ½,0, - ½ or 1. The core and delta point is predicted when the Poincare Index value is ½ and -½, respectively.

Only after the core point has been identified and proven legitimate, other minutiae, such as ridge ending and the bifurcation, may be easily tracked, taking the core point as a reference. It is necessary to apply pre-processing filters to the input image, such as 2-D adaptive wiener filters 2-D median, and improve image quality by decreasing noise and extracting other minutia's points as quickly and reliably as possible. After improving the image's quality in the pre-processing step, the minutia extraction process begins by converting the image to a binarized image. This is achieved by setting the intensity value of the each pixel to 1 if the pixel intensity is higher than the mean intensity value of the current block to which the pixel belongs. Skeletonization is an effective pre-processing method used on the image again after binarization. It is possible to achieve skeletonization, sometimes known as thinning, by decreasing the width of all of the ridgelines to one pixel thick, which allows you to see the whole pattern as one single line skeletal view. Following the fingerprint ridges' thinning, the following step is to mark locations of minutia on the fingerprint. As the frequency of minutiae identified increases, the likelihood of getting an accurate result increase. The concept of Crossing Number (C.N.) is frequently employed to obtain minute details. For a pixel, P crossing number is specified by Rutovitz as

$$C_n(P) = \frac{1}{2}\sum_{i=1}^{8} |P_i - P_{i+1}| \quad (4)$$

The binary pixel intensity value in the neighbourhood of P is represented by Pi=(0 or 1) and P1=P9. If we take a specific point P as an example, the crossing number Cn(P) is equal to half the sum of all the subsequent differences among pairs of neighbouring pixels in P's eight neighbourhood. The crossing number attributes of a ridge pixel can be used to determine whether a pixel is an ending, bifurcation, or non-minutia point.

If Cn(P) = = 1, then the ridge has reached its end, and in case of Cn(P) = = 3, then the ridge has reached its bifurcation. As ridge ends and ridge bifurcations are given greater attention, this is the best circumstance, and no need to take into consideration. Cn(P) > 3 because it is a crossing point, so this is the best possible situation. Following minutia marking, the image should be subjected to a minutia post-processing stage, as the preliminary phases would have included a significant amount of fictitious minutia. Below is a list of the numerous rules that may be used to eliminate incorrect details from images.

Rule 1). If the distance between a bifurcation and a termination is less than D, and if the two minutiae are positioned on the very same ridge, **THEN** in this case both of them should be eliminated from consideration.

Rule 2). **IF** the distance between any two bifurcations is less than D and they are both in the same ridge, **THEN** delete the minutia that appears to be two bifurcations that really are difficult to differentiate.

Rule 3). IF the distance between any two terminations is smaller than D, **THEN** minutiae are eliminated.

Rule 4). **IF** two terminations are within a distance D of one another but positioned on opposite ridges, and their directions synchronized with a minimal angle fluctuation, and there is no other termination between those two terminations. **THEN** delete both of the terminations.

Where **D** is the Euclidean Distance, which in this case is 6 pixels in this study

The image would still contain numerous minutiae required to construct a unique string even after removing the false minutiae. Only minutia points that are unique in the region of interest of the core point are considered. It is now possible to capture all the minutia, including termination and bifurcation, using a position coordinate and an orientation angle. The x-axes and y-axes and orientation angle define the location of the minutia points in the fingerprint. The minutiae points retrieved from the region of interest are reshaped in the NX3 matrix containing x, y, axis of minutiae and orientation angles. This matrix after that is converted into a unique string. Once the fingerprint features from the finger provided by the user at the time of authentication are extracted and converted into a unique string, the string undergoes a series of steps to generate a one-time password(OTP), as shown in fig 4. The algorithm of one-time-password (OTP) formation proceeds as follows:

1. The user registers their fingerprints with the server through the mobile application, and these fingerprints will be used as the first seed for the generation of the one-time password (OTP).
2. The user's live fingerprint is obtained through a mobile application during the authentication process.
3. The OTP module extracts the fingerprint's features and turns them into a unique string using the features of the fingerprint. The procedure for feature extraction and the unique string creation from fingerprint have already been explained above.
4. The string obtained from fingerprint features serves as the seed for generating the OTP code.
5. The string obtained from fingerprint features is passed to RIPMED160 for hash generation, resulting in the generation of a 160-bit hash. The RIPEMD160 is chained N times to generate a secure hash; in this case, N is the value of the challenge sent by the authentication server. The use of RIPEMD 160 would provide two unique advantages: a) A 160-bit hash value is more secure. b) In a prior standard, TOTP defined the Dynamic Truncation method for producing 6-digit OTP numbers from the 160-bit hash value. In spite of the fact that SHA 1 is the most extensively adopted hash algorithm for 160-bit hashes, it is theoretically susceptible to an attack. A more beneficial alternative is thus presented by RIPEMD 160 in this situation.
6. When using the RIPEMD160 to generate a 160-bit hash, the hash is shortened to reduce the 160-bit hash to just a string of four-bytes.
7. The 4-byte string is converted into one-time password (OTP) of 6- or 8-digits.

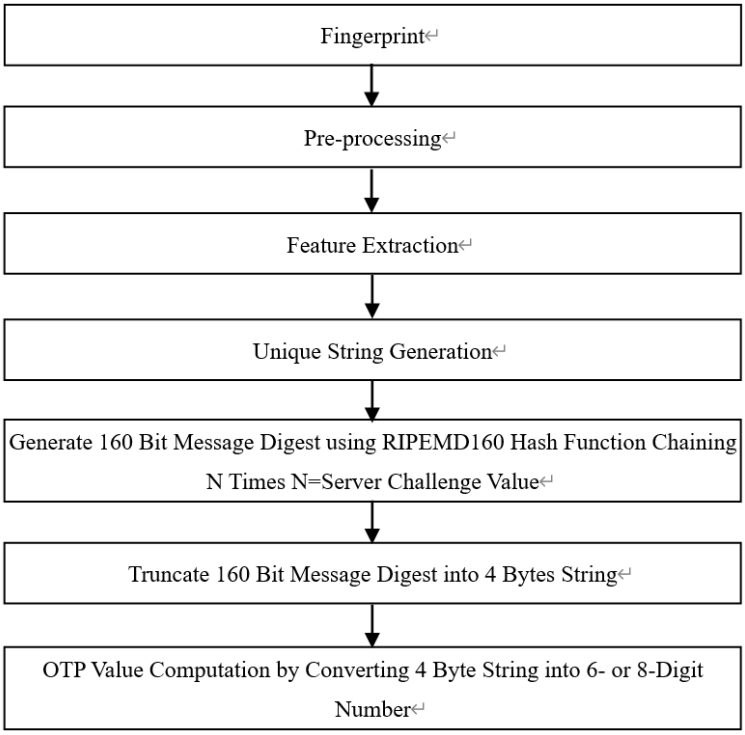

Fig.4. Proposed One-Time-Password Generation Process

4. Experiment Results

A client-server-based software application was developed to evaluate the proposed authentication scheme's performance and benefits and limitations. To allow it to be used on any mobile device running the Android operating system, the server application was created in Java and the client application in Android. The user registration and verification modules are contained within the client application; before usage, it is necessary to install it on the client-side of the smartphone. Firebase hosts the present experiment's programming module for creating one-time passwords (OTP) on the server-side and the database for storing fingerprint templates. The server-side application that generates OTP retrieves specific user fingerprint features from the database and uses the proposed OTP algorithm to generate OTP on the server. A controlled lab environment was used to conduct experiments with users of varying educational backgrounds and ages to determine whether the proposed authentication approach could provide satisfactory recognition performance under the circumstances. There was a total of 35 participants who took part in the study; they included students of the university, professors, and non-teaching staff who were all familiar with smartphone applications. Instruction was given to the participants in hands-on practice on installing the mobile application for the registration process and verification and using the proposed authentication mechanism on the smartphone. A mere five authentication attempts were allowed to each participant to assess the proposed system authentication performance

following registration, with each user being allowed a mere five authentication attempts. When the proposed authentication scheme was tested against the biometric evaluation criteria Failure to Enroll (FTE), True Acceptance Rate (TAR), False Rejection Rejection Rate (FRR), True Rejection Rate (TRR), and False Acceptance Rate (FAR), the findings achieved in the proposed authentication scheme on the threshold of 75% are depicted in the following graph.

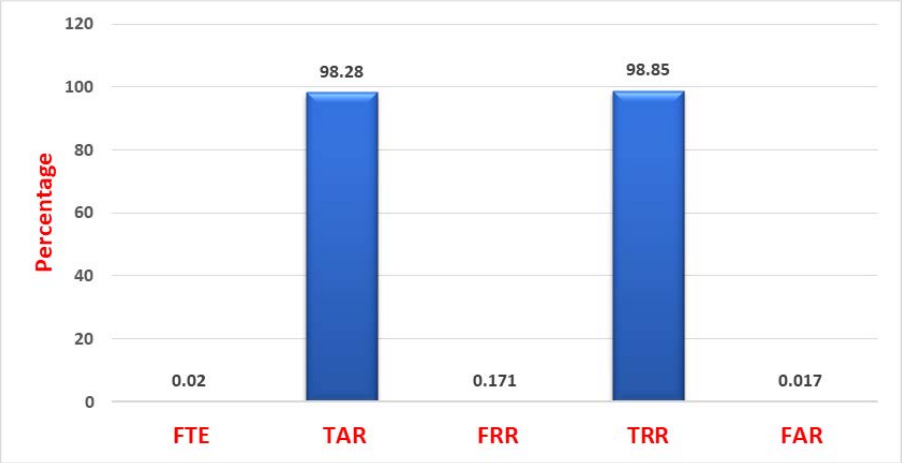

Fig.5. Performance Evaluation of Proposed Authentication Scheme

The proposed biometric-based authentication results are shown graphically in Fig.5. It shows that the values of the biometric performance evaluation parameters are good; in this way, the proposed scheme is appropriate for real-time biometric-based access control systems in mobile environments involving client-server architecture. The proposed authentication scheme uses fingerprint features to authenticate a valid user utilizing mobile phones to access sensitive internet services. It is critical to determine this authentication technique's usability before implementing it in practice. For this reason, a usability assessment of the proposed authentication scheme was carried out.

The primary purpose of the usability evaluation of the proposed authentication scheme was to arrive at a usability conclusion that could be employed in potential improvements. To evaluate the usefulness of the proposed authentication scheme, measures from previous research ISO-9241-11 [86] were selected and utilized to assess its usability. According to these criteria, the essential usability aspects in a specific context are effectiveness, efficiency, and user satisfaction with the product or service. The mobile application developed generated several important activity logs, which were utilized to measure the efficiency and effectiveness by storing the time spent enrolling and validating each user by the proposed authentication scheme. Each of the five trials in the experiment required participants to authenticate themselves using a verification module, which they were advised to do in each trial. It was necessary to quantify the five experiments' qualitative outcomes to determine their efficiency and efficacy. The time it takes to accomplish a task is used to determine the efficiency of a process. The following formulas were used to determine the efficiency of the proposed authentication scheme's registration and verification processes.

$$\mathbf{Av(R)} = \frac{\text{Sum (Successful Registration Times)}}{\text{Number of Successful Registrations}}$$

$$\mathbf{Av(V)} = \frac{\text{Sum (Successful Login Times)}}{\text{Number of Successful Logins}}$$

Results are shown in the graph revealed that the maximum time is required to register and verify users in the current study is 11 and 12 seconds while a minimum of 4 and 6 seconds, respectively. These results indicate how efficiently and quickly the proposed system can be used for authentication, demonstrating its effectiveness. Effectiveness is another essential usability evaluation parameter that indicates the accuracy and correctness of achieving defined goals. In context to the current study, effectiveness can be described as the ability of a biometric system to enrol and verify users, and it is typically stated in terms of success rate, also known as completion rate. The number of errors made during the verification/enrollment process. If a legitimate user is authenticated through a legitimate login attempt, the effectiveness is measured as the total number of successful login attempts across all of the login attempts during the authentication process of the legitimate user. For the current study, 35 users have registered; the effectiveness of the proposed method is measured by taking into account the five attempts made by each user. The success rate of a login attempt is calculated as follows.

$$\text{S. R. (L)} = \frac{\text{Number of Successful Logins}}{\text{Number of Total Logins}}$$

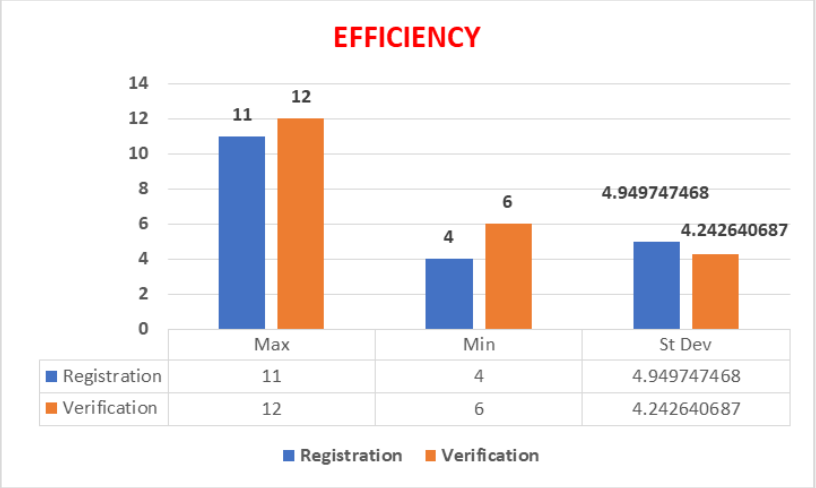

Fig.6. Efficiency of the Proposed Authentication Scheme

Fig.7. Effectiveness of the Proposed Authentication Scheme

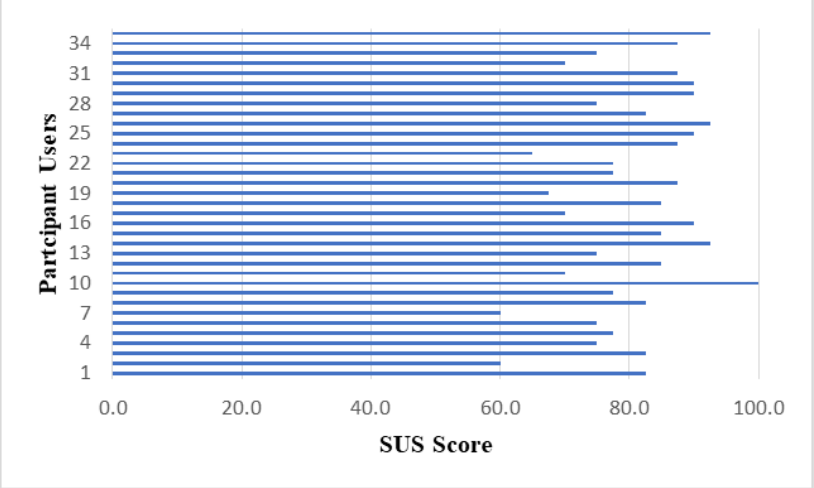

Fig.8. System Usability Scale Score for Proposed Authentication Scheme

According to the findings, as illustrated in Fig. 7, the successful login rate is incredibly high; 98.28 percent of registered users appeared to be able to authenticate themselves successfully without experiencing any issues, and only 1.71 percent of registered users failed to login due to an error in which the fingerprint scanned by the mobile application did not match the template of the fingerprint kept on the server. Consequently, the OTP produced on the client and the OTP produced on the server did not relate.

Questionnaires were distributed to all of the 35 registered users who took part in the current study to measure perceptions of apparent usability after the registered legitimate users had completed all authentication attempts. The subjective feelings of the user are taken into consideration when determining user satisfaction, which describes the comfortability and significance of the application, among many other things. This is in conversely to efficiency and effectiveness. To test user satisfaction with the current system, the System Usability Scale (SUS) [87–89] has been utilized, and it was discovered to be highly effective. Using a Likert 10-item measure based on forced-choice questions, the SUS presents a global picture of people's subjective opinions about usability evaluation. It is often used after a user had the chance to interact with the service somehow. The SUS score measures its effectiveness, efficiency, and overall ease of use, ranging from 0-100. In response to the questions presented in the questionnaire, the SUS score for the proposed authentication scheme is calculated based on the answers. According to the chart below, both the individual and overall, SUS scores were computed in the same way. Under the condition of an acceptable adjective rating, a SUS score of 80.6 has been achieved for the proposed authentication technique, indicating that it is feasible.

5. Conclusion

Mobile consumers are becoming more interested in online internet services such as financial transactions, e-commerce, and other such services as the use of smartphones increases. Strong authentication is required to protect access to these services through smartphones. Relying on traditional authentication mechanisms based on knowledge in an increasingly mobile environment is proven to be unsustainable. Recent advancements in the mobile technology environment, such as the mass production of smartphones equipped with fingerprint sensors biometric authentication, is becoming an increasingly attractive alternative to traditional knowledge and token-based authentications. Incorporating biometrics into consumer-facing mobile application authentication is becoming an increasingly important business need since it provides both simplicities of use and increased security. This paper proposed a new fingerprint-based authentication mechanism that may be utilized in smartphones using the challenge-response method. The proposed authentication method prevents common attacks such as Man-in-the-Middle attacks, password guessing, and replay attacks and mitigates additional vulnerabilities such as MITPhone, SIM Swap attacks, and other SMS-based OTP authentication threats.

Furthermore, in the current work, an OTP computational process that is both secure and user-friendly has been proposed, which overcomes the constraints of existing OTP generating techniques based on time synchronization and mathematical algorithms, respectively. The preliminary findings of the performance and usability analysis of the proposed authentication system indicate that the proposed authentication scheme provides a high level of efficiency, effectiveness, and user satisfaction to its users; therefore, the proposed authentication method is suited for use in mobile contexts.

References

[1] O. O. Ajaegbu, C. Ajaegbu, and O. Adewunmi S, “Smartphone Technological Advancement Trends: A Scheme for Knowledge Acquisition Towards Societal Development,” *Inf. Technol. J.*, vol. 18, no. 1, pp. 1–7, 2018, doi: 10.3923/itj.2019.1.7.

[2] A. Shah, P. Roongta, C. Jain, V. Kaushik, and A. Awadhiya, “Digital Payments 2020: The Making of $500 Billion Ecosystem in India,” pp. 1–52, 2016, [Online]. Available: https://image-src.bcg.com/BCG_COM/BCG-Google Digital Payments 2020-July 2016_tcm21-39245.pdf.

[3] T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, “A critical insight into the identity authentication systems on smartphones,” in *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 13, no. 3, 2019, pp. 982–989.

[4] R. Amin, T. Gaber, G. Eltaweel, and A. E. Hassanien, “Biometric and traditional mobile authentication techniques: Overviews and open issues,” in *Intelligent Systems Reference Library*, Intelligen., vol. 70, Springer, 2015, pp. 423–446.

[5] W. H. Lee and R. Lee, “Implicit sensor-based authentication of smartphone users with smartwatch,” *ACM Int. Conf. Proceeding Ser.*, vol. 18-June-20, 2016, doi: 10.1145/2948618.2948627.

[6] S. J. Wang and J. F. Chang, “Smart card based secure password authentication scheme,” *Comput. Secur.*, vol. 15, no. 3, pp. 231–237, 1996, doi: 10.1016/0167-4048(96)00005-3.

[7] J. Jeong, M. Y. Chung, and H. Choo, “Integrated OTP-Based User Authentication and Access Control Scheme in Home Networks,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 4773 LNCS, pp. 123–133, 2007, doi: 10.1007/978-3-540-75476-3_13.

[8] O. Ogbanufe and D. J. Kim, “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment,” *Decis. Support Syst.*, vol. 106, pp. 1–14, 2018, doi: 10.1016/J.DSS.2017.11.003.

[9] P. Sealy, “Get smart: why biometric cards will reshape the payments industry,” *Biometric Technol. Today*, vol. 2018, no. 8, pp. 5–8, 2018.

[10] A. Qusef, A. Albadarneh, S. Elish, and M. Muhanna, “Mitigating personalization challenges in mobile commerce: An empirical study,” *Comput. Electr. Eng.*, vol. 89, 2021.

[11] A. De Keyser, Y. Bart, X. Gu, S. Q. Liu, S. G. Robinson, and P. K. Kannan, “Opportunities and challenges of using biometrics for business: Developing a research agenda,” *J. Bus. Res.*, vol. 136, pp. 52–62, 2021.

[12] C. G. Deborah Golden, “Addressing Cyber Threats Multi-Factor Authentication for Privileged User Accounts Contents,” 2015. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-federal-cyber-mfa-pov.pdf.

[13] M. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, “Authentication schemes for smart mobile devices: threat models, countermeasures, and open research issues,” *Telecommun. Syst.*, vol. 73, no. 2, pp. 317–348, 2020, doi: 10.1007/s11235-019-00612-5.
[14] N. A. Lal, S. Prasad, and M. Farik, “A Review Of Authentication Methods,” vol. 5, no. 11, pp. 246–249, 2016.
[15] S. Laitos, “Biometrics As an Alternative To Passwords for Older Users,” 2015.
[16] L. O’Gorman, “Comparing passwords, tokens, and biometrics for user authentication | Bipin Kumar - Academia.edu,” vol. 91, no. 12, pp. 2021–2040, 2005, [Online]. Available: http://www.academia.edu/654335/Comparing_passwords_tokens_and_biometrics_for_user_authentication.
[17] J. N. Oruh, “Three-Factor Authentication for Automated Teller Machine System,” no. December 2014, 2021.
[18] K. R. Reese, “Evaluating the Usability of Two-Factor Authentication,” 2018.
[19] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, “Biometric Authentication on iPhone and Android: Usability, Perceptions, and Influences on Adoption,” 2015, doi: 10.14722/usec.2015.23003.
[20] D. H. Shih, C. M. Lu, and M. H. Shih, “A flick biometric authentication mechanism on mobile devices,” *ICCSS 2015 - Proc. 2015 Int. Conf. Inf. Cybern. Comput. Soc. Syst.*, pp. 31–33, 2015, doi: 10.1109/ICCSS.2015.7281144.
[21] R. Spolaor, Q. Q. Li, M. Monaro, M. Conti, L. Gamberini, and G. Sartori, “Biometric authentication methods on smartphones: A survey,” *PsychNology J.*, vol. 14, no. 2–3, pp. 87–98, 2016.
[22] N. A. Albahbooh and P. Bours, “A mobile phone device as a biometrics authentication method for an ATM terminal,” in *Proceedings - 15th IEEE International Conference on Computer and Information Technology, CIT 2015*, 2015, pp. 2017–2024, doi: 10.1109/CIT/IUCC/DASC/PICOM.2015.299.
[23] F. Karegar, J. S. Pettersson, and S. Fischer-Hübner, “Fingerprint recognition on mobile devices: Widely deployed, rarely understood,” *ACM Int. Conf. Proceeding Ser.*, 2018, doi: 10.1145/3230833.3234514.
[24] B. Abazi, B. Qeliaja, and E. Hajrizi, “Application of biometric models of authentication in mobile equipment,” *IFAC-PapersOnLine*, vol. 52, no. 25, pp. 543–546, 2019, doi: 10.1016/j.ifacol.2019.12.602.
[25] T. W. Paper, “TECHNICAL WHITE PAPER ENABLING BIOMETRICS FOR MOBILE APPLICATION Comparing Nok Nok S3 Authentication ENABLING BIOMETRICS FOR MOBILE APPLICATION AUTHENTICATION.”
[26] T. Update, “Biometric Authentication : IRIS image Capture , Storage and Processing,” no. January, pp. 31–33, 2012.
[27] A. K. Tiwari, R. Agarwal, and S. Goyal, “Biometric Authentication for Mobile Banking Security,” *SSRN Electron. J.*, no. September, 2014, doi: 10.2139/ssrn.2438213.
[28] S. P. A. K. Jain, r. Bolle, *Biometrics: Personal Identification in Networked Security*. 1999.
[29] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics Handbook of Biometrics*. 2007.
[30] Vic Berger, “Biometrics Security Technology: The Future Now,” 2007.
[31] S. Wang and J. Liu, “Biometrics on mobile phone,” *Recent Appl. Biometrics*, 2011, doi: 10.5772/17151.
[32] G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, and I. Martinovic, “Mobile Biometrics in Financial Services: A Five Factor Framework,” 2017, [Online]. Available: https://www.cs.ox.ac.uk/files/9113/Mobile Biometrics in Financial Services.pdf.
[33] Leila Zoubida, Réda Adjoudj,"Integrating Face and the Both Irises for Personal Authentication", International Journal of Intelligent Systems and Applications, Vol.9, No.3, pp.8-17, 2017.
[34] Vanaja Roselin.E.Chirchi, Laxman.M.Waghmare,"Iris Biometric Authentication used for Security Systems", International Journal of Image, Graphics and Signal Processing, vol.6, no.9, pp.54-60, 2014.
[35] Khaja Mizbahuddin Quadry, A Govardhan, Mohammed Misbahuddin, "Design, Analysis, and Implementation of a Two-factor Authentication Scheme using Graphical Password", International Journal of Computer Network and Information Security, Vol.13, No.3, pp.39-41, 2021.
[36] S. Trewin, C. Swart, L. Koved, J. Martino, K. Singh, and S. Ben-David, “Biometric authentication on a mobile device,” p. 159, 2012, doi: 10.1145/2420950.2420976.
[37] R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior, *Guide to Biometrics*. 2004.
[38] J. Wayman, A. Jain, D. Maltoni, and D. Maio, “An Introduction to Biometric Authentication Systems,” *Biometric Syst.*, pp. 1–20, 2005, doi: 10.1007/1-84628-064-8_1.
[39] S. Sanderson and J. H. Erbetta, “Authentication for secure environments based on Iris scanning technology,” *IEE Colloq.*, no. 18, pp. 53–59, 2000, doi: 10.1049/IC:20000468.
[40] A. Bal and A. Acharya, “Biometric authentication and tracking system for online examination system,” *2011 Int. Conf. Recent Trends Inf. Syst. ReTIS 2011 - Proc.*, pp. 209–213, 2011, doi: 10.1109/RETIS.2011.6146869.
[41] A. Laghari, W. Waheed-Ur-Rehman, and Z. A. Memon, “Biometric authentication technique using smartphone sensor,” *Proc. 2016 13th Int. Bhurban Conf. Appl. Sci. Technol. IBCAST 2016*, pp. 381–384, 2016, doi: 10.1109/IBCAST.2016.7429906.
[42] J. L. WAYMAN, “FUNDAMENTALS OF BIOMETRIC AUTHENTICATION TECHNOLOGIES,” *http://dx.doi.org/10.1142/S0219467801000086*, vol. 01, no. 01, pp. 93–113, 2011, doi: 10.1142/S0219467801000086.
[43] Q. Tao and R. Veldhuis, “Biometric authentication system on mobile personal devices,” *IEEE Trans. Instrum. Meas.*, vol. 59, no. 4, pp. 763–773, 2010, doi: 10.1109/TIM.2009.2037873.
[44] A. Mahfouz, T. M. Mahmoud, and A. S. Eldin, “A survey on behavioral biometric authentication on smartphones,” *J. Inf. Secur. Appl.*, vol. 37, pp. 28–37, 2017, doi: 10.1016/J.JISA.2017.10.002.
[45] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, “Security and Accuracy of Fingerprint-Based Biometrics: A Review,” *Symmetry 2019, Vol. 11, Page 141*, vol. 11, no. 2, p. 141, 2019, doi: 10.3390/SYM11020141.
[46] S. Jabin and F. J. Zareen, “Biometric signature verification,” *Int. J. Biom.*, vol. 7, no. 2, pp. 97–118, 2015, doi: 10.1504/IJBM.2015.070924.
[47] A. El-Sisi, “Design and Implementation Biometric Access Control System Using Fingerprint for Restricted Area Based on Gabor Filter,” *Int. Arab J. Inf. Technol.*, vol. 8, no. 4, 2011.
[48] V. Conti, M. Collotta, G. Pau, and S. Vitabile, “Usability analysis of a novel biometric authentication approach for android-based mobile devices,” *J. Telecommun. Inf. Technol.*, vol. 2014, no. 4, pp. 34–43, 2014.

[49] S. Sawarkar, "Finger Print Matching Algorithm for Android," *Int. J. Eng. Res. Technol.*, vol. 02, no. 10, pp. 3819–3823, 2013, [Online]. Available: www.ijert.org.
[50] J. Hu, L. Peng, and L. Zheng, "XFace: A Face Recognition System for Android Mobile Phones," *Proc. - 3rd IEEE Int. Conf. Cyber-Physical Syst. Networks, Appl. CPSNA 2015*, pp. 13–18, 2015, doi: 10.1109/CPSNA.2015.12.
[51] M. De Marsico, C. Galdi, M. Nappi, and D. Riccio, "FIRME: Face and iris recognition for mobile engagement," *Image Vis. Comput.*, vol. 32, no. 12, pp. 1161–1172, 2014, doi: 10.1016/J.IMAVIS.2013.12.014.
[52] G. Lovisotto, R. Malik, I. Sluganovic, M. Roeschlin, P. Trueman, and I. Martinovic, "Mobile Biometrics in Financial Services: A Five Factor Framework."
[53] L. Fridman, S. Weber, R. Greenstadt, and M. Kam, "Active Authentication on Mobile Devices via Stylometry, Application Usage, Web Browsing, and GPS Location," *IEEE Syst. J.*, vol. 11, no. 2, pp. 513–521, 2017, doi: 10.1109/JSYST.2015.2472579.
[54] E. B. Fernandez, M. M. Larrondo-Petrie, and A. E. Escobar, "Contexts and context-based access control," *Third Int. Conf. Wirel. Mob. Commun. 2007, ICWMC '07*, pp. 73–78, 2007, doi: 10.1109/ICWMC.2007.30.
[55] C. J. Tsai, C. C. Peng, M. L. Chiang, T. Y. Chang, W. J. Tsai, and H. S. Wu, "Work in progress: A new approach of changeable password for keystroke dynamics authentication system on smart phones," *Proc. 2014 9th Int. Conf. Commun. Netw. China, CHINACOM 2014*, pp. 353–356, 2015, doi: 10.1109/CHINACOM.2014.7054316.
[56] C. C. Teo and H. F. Neo, "Behavioral fingerprint authentication: The next future," *ACM Int. Conf. Proceeding Ser.*, vol. Part F128534, pp. 1–5, 2017, doi: 10.1145/3093293.3093296.
[57] K. B. Raja, R. Raghavendra, M. Stokkenes, and C. Busch, "Multi-modal authentication system for smartphones using face, iris and periocular," *Proc. 2015 Int. Conf. Biometrics, ICB 2015*, no. June, pp. 143–150, 2015, doi: 10.1109/ICB.2015.7139044.
[58] M. Said, K. Mohamed, A. Elshenawy, and M. EZZ, "A SURVEY ON SMARTPHONE PROTECTING IDENTIFICATION AGAINST ATTACKS USING BIOMETRIC AUTHENTICATION SYSTEMS," *J. Al-Azhar Univ. Eng. Sect.*, vol. 16, no. 59, pp. 288–299, 2021, doi: 10.21608/AUEJ.2021.166649.
[59] M. A. S. Bubukayr and M. A. Almaiah, "Cybersecurity Concerns in Smart-phones and applications: A survey," in *2021 International Conference on Information Technology (ICIT)*, 2021, pp. 725–731, doi: 10.1109/ICIT52682.2021.9491691.
[60] D. Kunda and M. Chishimba, "A Survey of Android Mobile Phone Authentication Schemes," *Mob. Networks Appl. 2018*, pp. 1–9, 2018, doi: 10.1007/S11036-018-1099-7.
[61] L. M. Mayron, "Biometric Authentication on Mobile Devices," *IEEE Secur. Priv.*, vol. 13, no. 3, pp. 70–73, 2015, doi: 10.1109/MSP.2015.67.
[62] Q. Su, J. Tian, X. Chen, and X. Yang, "A Fingerprint Authentication System Based on Mobile Phone," *Lect. Notes Comput. Sci.*, vol. 3546, pp. 151–159, 2005, doi: 10.1007/11527923_16.
[63] S. S. Mudholkar, "Biometrics Authentication Technique for Intrusion Detection Systems Using Fingerprint Recognition," *Int. J. Comput. Sci. Eng. Inf. Technol.*, vol. 2, no. 1, pp. 57–65, 2012, doi: 10.5121/IJCSEIT.2012.2106.
[64] F. Karegar, J. S. Pettersson, S. Fischer-Hübner, and S. Fischer, "Fingerprint Recognition on Mobile Devices: Widely Deployed, Rarely Un-derstood," 2018, doi: 10.1145/3230833.3234514.
[65] B. A. Oke, O. M. Olaniyi, A. A. Aboaba, and O. T. Arulogun, "Multifactor authentication technique for a secure electronic voting system," *Electron. Gov.*, vol. 17, no. 3, pp. 312–338, 2021, doi: 10.1504/EG.2021.115999.
[66] J. Priesnitz, C. Rathgeb, N. Buchmann, C. Busch, and M. Margraf, "An overview of touchless 2D fingerprint recognition," *Eurasip J. Image Video Process.*, vol. 2021, no. 1, 2021, doi: 10.1186/S13640-021-00548-4.
[67] Y. H. Jo, S. Y. Jeon, J. H. Im, and M. K. Lee, "Security analysis and improvement of fingerprint authentication for smartphones," *Mob. Inf. Syst.*, vol. 2016, 2016, doi: 10.1155/2016/8973828.
[68] V. Matyáš and Z. Říha, "Biometric Authentication — Security and Usability," no. April 2016, pp. 227–239, 2002, doi: 10.1007/978-0-387-35612-9_17.
[69] E. Pagnin and A. Mitrokotsa, "Privacy-Preserving Biometric Authentication: Challenges and Directions," 2017, doi: 10.1155/2017/7129505.
[70] E. Marasco and B. Cukic, "Privacy protection schemes for fingerprint recognition systems," *Biometric Surveill. Technol. Hum. Act. Identif. XII*, vol. 9457, p. 94570D, 2015, doi: 10.1117/12.2178978.
[71] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognit.*, vol. 78, pp. 242–251, 2018, doi: 10.1016/J.PATCOG.2018.01.026.
[72] C. Kauba *et al.*, "Towards Using Police Officers' Business Smartphones for Contactless Fingerprint Acquisition and Enabling Fingerprint Comparison against Contact-Based Datasets," *Sensors MDPI*, vol. 21, no. 7, 2021, doi: 10.3390/s21072248.
[73] S. K. Ganiyev and Z. T. Khudoykulov, "Biometric cryptosystems: Open issues and challenges," *2016 Int. Conf. Inf. Sci. Commun. Technol. ICISCT 2016*, 2016, doi: 10.1109/ICISCT.2016.7777408.
[74] J. N. Pato and L. I. Millett, "Biometric recognition: Challenges and opportunities," *Biometric Recognit. Challenges Oppor.*, pp. 1–182, 2010, doi: 10.17226/12720.
[75] R. Bansal, P. Sehgal, and P. Bedi, "Minutiae Extraction from Fingerprint Images-a Review," *IJCSI Int. J. Comput. Sci.*, 2011, [Online]. Available: www.IJCSI.org.
[76] M. M. H. Ali, V. H. Mahale, P. Yannawar, and A. T. Gaikwad, "Overview of fingerprint recognition system," *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 1334–1338, 2016, doi: 10.1109/ICEEOT.2016.7754900.
[77] U. Rajanna, A. Erol, and G. Bebis, "A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion," *Pattern Anal. Appl. 2009 133*, vol. 13, no. 3, pp. 263–272, 2009, doi: 10.1007/S10044-009-0160-3.
[78] P. Gnanasivam and S. Muttan, "An efficient algorithm for fingerprint preprocessing and feature extraction," *Procedia Comput. Sci.*, vol. 2, pp. 133–142, 2010, doi: 10.1016/J.PROCS.2010.11.017.
[79] R. Kaur, P. S. Sandhu, and A. Kamra, "A novel method for fingerprint feature extraction," *ICNIT 2010 - 2010 Int. Conf. Netw. Inf. Technol.*, pp. 1–5, 2010, doi: 10.1109/ICNIT.2010.5508569.
[80] S. A. Lone and A. H. Mir, "A stable and secure one-time-password generation mechanism using fingerprint features," *Int. J.*

Innov. Technol. Explor. Eng., vol. 8, no. 9, pp. 2431–2438, 2019, doi: 10.35940/ijitee.i8919.078919.
[81] G. B. Iwasokun and O. C. Akinyokun, "Fingerprint Singular Point Detection Based on Modified Poincare Index Method," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 7, no. 5, pp. 259–272, 2014, doi: 10.14257/ijsip.2014.7.5.23.
[82] F. Magalhães, H. P. Oliveira, and A. C. Campilho, "A new method for the detection of singular points in fingerprint images," in *2009 Workshop on Applications of Computer Vision, WACV 2009*, 2009, pp. 0–5, doi: 10.1109/WACV.2009.5403106.
[83] V. Conti, "Biometric Authentication Overview: a Fingerprint Recognition Sensor Description," *Int. J. Biosens. Bioelectron.*, vol. 2, no. 1, pp. 26–31, 2017, doi: 10.15406/ijbsbe.2017.02.00011.
[84] D. Zabala-Blanco, M. Mora, R. J. Barrientos, R. Hernández-García, and J. Naranjo-Torres, "Fingerprint classification through standard and weighted extreme learning machines," *Appl. Sci.*, vol. 10, no. 12, 2020, doi: 10.3390/APP10124125.
[85] R. Kumar, "Orientation Local Binary Pattern Based Fingerprint Matching," *SN Comput. Sci.*, vol. 1, no. 2, 2020, doi: 10.1007/s42979-020-0068-y.
[86] Y. Li, M. Mandal, and C. Lu, "Singular point detection based on orientation filed regularization and poincaré index in fingerprint images," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2013, pp. 1439–1443, doi: 10.1109/ICASSP.2013.6637889.
[87] J. Brooke, "SUS: a "quick and dirty'usability," in *Usability evaluation in industry*, 1996, pp. 189–194.
[88] Jeff Sauro, "MeasuringU: Measuring Usability with the System Usability Scale (SUS)," 2011. https://measuringu.com/sus/.
[89] N. Thomas, "How To Use The System Usability Scale (SUS) To Evaluate The Usability Of Your Website - Usability Geek." 2020, [Online]. Available: https://usabilitygeek.com/how-to-use-the-system-usability-scale-sus-to-evaluate-the-usability-of-your-website/.

Authors' Profiles

Mr Sajaad Ahmed is a research scholar at the Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Jammu and Kashmir, India. He received his master's in information technology from Guru Gobind Singh Indraprastha University, New Delhi, India. His research interests include network security and image processing.

Dr. Ajaz Hussain Mir is a Professor in the Department of Electronics and Communication Engineering at the National Institute of Technology, Srinagar. He received his BE in Electrical Engineering with a specialization in Electronics and Communication Engineering. He received his MTech and PhD in Computer Technology from the IIT Delhi (India) in 1989 and 1996. He is a Chief Investigator of the Ministry of Communication and Information Technology, Govt. of India project: Information Security Education and Awareness (ISEA). He has been guiding PhD and MTech theses in digital image processing, computer networks and other related areas and has published research in international journals of repute. His areas of interest are biometrics, image processing, security, wireless communication and networks.

How to cite this paper: Sajaad Ahmed Lone, A.H. Mir, "Smartphone-based Biometric Authentication Scheme for Access Control Management in Client-server Environment", International Journal of Information Technology and Computer Science(IJITCS), Vol.14, No.4, pp.34-47, 2022. DOI:10.5815/ijitcs.2022.04.04