A novel OTP based tripartite authentication scheme

Article *in* International Journal of Pervasive Computing and Communications · August 2021

DOI: 10.1108/IJPCC-04-2021-0097

CITATIONS
9

READS
408

2 authors:

Sajaad Ahmed
Islamic University of Science and Technology
26 PUBLICATIONS **136** CITATIONS
SEE PROFILE

Ajaz Hussain Mir
National Institute of Technology Srinagar
67 PUBLICATIONS **388** CITATIONS
SEE PROFILE

A novel OTP based tripartite authentication scheme

Sajaad Ahmed Lone
Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Srinagar, India, and

Ajaz Hussain Mir
Department of Electronics and Communication Engineering, National Institute of Technology Srinagar, Srinagar, India

Received 19 April 2021
Revised 10 July 2021
Accepted 10 July 2021

Abstract

Purpose – Because of the continued use of mobile, cloud and the internet of things, the possibility of data breaches is on the increase. A secure authentication and authorization strategy is a must for many of today's applications. Authentication schemes based on knowledge and tokens, although widely used, lead to most security breaches. While providing various advantages, biometrics are also subject to security threats. Using multiple factors together for authentication provides more certainty about a user's identity; thus, leading to a more reliable, effective and more difficult for an adversary to intrude. This study aims to propose a novel, secure and highly stable multi-factor one-time password (OTP) authentication solution for mobile environments, which uses all three authentication factors for user authentication.

Design/methodology/approach – The proposed authentication scheme is implemented as a challenge-response authentication where three factors (username, device number and fingerprint) are used as a secret key between the client and the server. The current scheme adopts application-based authentication and guarantees data confidentiality and improved security because of the integration of biometrics with other factors and each time new challenge value by the server to client for OTP generation.

Findings – The proposed authentication scheme is implemented on real android-based mobile devices, tested on real users; experimental results show that the proposed authentication scheme attains improved performance. Furthermore, usability evaluation proves that proposed authentication is effective, efficient and convenient for users in mobile environments.

Originality/value – The proposed authentication scheme can be adapted as an effective authentication scheme to accessing critical information using android smartphones.

Keywords Usability, Biometrics, Authentication, Fingerprint, Multifactor, OTP, Poincare index

Paper type Research paper

1. Introduction

In today's world, due to widespread adaptation of smart devices in major retail chains, banks, health insurers, state federal government agencies have become victims of data breaches by putting at risk the sensitive information of millions of citizens and customers. With the continued rapid expansion of data created by the combination of mobile, cloud computing technology, the internet of things, persistent computing, the breach into their data vaults can also increase. Strong authentication and authorization strategy of users is becoming a must for many applications today for securing confidential, classified and sensitive information. To connect a person with existing credentials, three modes of authentication are currently available, namely, knowledge: Individuals with specific knowledge such as passwords and phrases can access the service. Possession: what an

International Journal of Pervasive Computing and Communications

1742-7371
DOI 10.1108/IJPCC-04-2021-0097

individual possesses, such as keys, passports and smart cards. Biometrics: Physiological and behavioral characteristics of a person such as fingerprints, iris, signature, voice, are unique and differentiates one person from another (Zulkarnain *et al.*, 2013; Lone and Mir, 2019). Authentication methods based on possession and knowledge are the most widely used methods for computers, the internet and email accounts. The issue with these two authentication methods is that they do not link a person to a more or less known established identity, and therefore, do not authenticate the enrolled person. Furthermore, most data breaches are caused by poor and compromised passwords, as users appear to behave carelessly by providing passwords that are simple and can be recalled instantly. Password sharing and reuse of passwords across multiple accounts add in its ineffectiveness sentry at a time when critical data is ever more susceptible to attack (Dwivedi and Thomas, 2009; Towhidi *et al.*, 2011; Lal *et al.*, 2016; Turn, 2020). Authentication based on biometrics often provides an extra layer of security as it is not possible to share the physiological or behavioral characteristics of a person. Biometrics is an intrinsic property of an individual. Therefore, biometric authentication offers a confident assurance about the authenticity of a person can be confidently and securely established, which possession and knowledge do not guarantee (Biometrics-Home, 2021; Bolle *et al.*, 2004; O'Gorman, 2005). All the authentication mechanisms discussed above are not created equal, so there is a need for strong authentication. For example, username and password are not secure, although it is the most common authentication method. Weak and stolen passwords result in most data breaches.

To palliate traditional authentication methods' weaknesses, multi-factor authentication (MFA) protocols combine two or more different factors to achieve reliable and robust authentication to access critical assets and resources. For example, MFA may be using a password combined with fingerprint recognition in authentication applications. For the most part, MFA is based on biometrics. Due to the widespread use of smartphones and declining technology costs, it has been possible to provide two or more factors easily. So, MFA should be a core part of the enterprise authentication strategy.

In this study, the development of a challenge-response authentication based on a one-time password (OTP) that uses all three authentication factors for authenticating legitimate users has been proposed. The following sections make up the paper. Section 2 provides a summary of relevant work, while Section 3 deliberates open problems with current structures. The proposed authentication scheme and the OTP generation algorithm are presented in Section 4. The proposed authentication scheme implementation and performance evaluation in Section 5 and usability analysis and conclusion are defined in Sections 6 and 7, respectively.

2. Background and related work

Many researchers have investigated numerous studies about various security and user authentication issues for accessing essential and highly confidential information. During the study of different methods used previously and in current systems, OTP use in authentication was found to provide greater security in access control in public and private networks (Mehraj *et al.*, 2015). The OTP is only valid for one access attempt when attempting to complete a unit of transactions. One of the more apparent benefits of using OTP is its fail-proof security against replay attacks, which ensures that a specific password created once can never be replicated a second time, rendering the password useless if it falls into the hands of an intruder. As a result, OTP has been studied to see whether there is a more straightforward way to enhance user authentication (Deore and Waghmare, 2016). Owing to the varied formats of OTP usage and the architecture developed by the past protocol makers and researchers, various OTP schemes have also been patented, but

standardization is a challenge. Various authentication schemes based on OTP are discussed in this section.

2.1 One-time password-based authentication methods

2.1.1 Hash-based message authentication code-based one-time password. HOTP is a hash-based message authentication code (HMAC)-based OTP algorithm that provides authentication by symmetrically generating one-time passwords that are only used for one authentication attempt, (Deore and Waghmare, 2016). In this type of OTP-based authentication, both authenticator and token share secret key (seed) and counter. Both parties use the default hash function SHA1 with the secret key and the counter to compute the HMAC-based one-time password (HOTP) value. The token displays the computed 160-bit value, which is then reduced to 6 or 8 decimal digits. The authenticator (Server) then compares the OTP value provided locally with the token's OTP value. The counter is incremented separately than by both parties. As HOTP does not have the time-based constraint, it is somewhat easier to use yet might be more susceptible to brute force attacks that is because of the long window in which HOTP is valid (Beikverdi and Tan, 2012; Mathews and Panchami, 2017; HMAC-based One-Time Password-Wikipedia, 2020).

2.1.2 Time-based one-time password. The time-based one-time password (TOTP) is a variant of the HMAC-based One-Time Password (HOTP) algorithm that generates an OTP using a secret key and the current time. The token includes an accurate clock that has been synchronized with the proprietary authentication server's clock in this type of authentication. To authenticate a token by the authenticator server, both use the secret key and current time as input to generate OTP value. The generated OTP value by the token is sent to the authenticator; the authenticator uses the same algorithm used by the token to generate OTP and the authenticator matches its OTP with the one sends by the token if both matches, then the user is considered as a legitimate user (Rydell *et al.*, 2011; Hassan *et al.*, 2020). Although TOTP is more secure than HOTP, the major weakness of this authentication method is it does not authenticate the users if the token and authenticator are unsynchronized; that is why TOTP has a limited lifespan after this period, the OTP value changes. The Google two-factor authenticator generates OTP using TOTP. As all TOTP systems depend on the user's phone's clock to match the server's clock, this Google authenticator becomes out of sync (Hassan *et al.*, 2020).

2.1.3 Challenge-response-based one-time password authentication. In this type of authentication mechanism, a user requesting access to a computer, network or other resources is authenticated based on a challenge or question presented by one entity (Server) and another entity (token) to be authenticated provides a valid response. A challenge-response-based involves a series of steps in which the secret key is initially shared between token and server before authentication. When the token is authenticated, the server sends a challenge value to the token (client). Both server and client use challenge value and secret key to generate OTP using a similar algorithm. The token sends the computed OTP to the server and compares it with locally generated OTP to check whether the user is legitimate. As the value used for the challenge by the server is uniquely generated by each time; thus making this type of authentication relatively secure. The challenge response-based authentication can defend against different attacks such as session reply attacks, reply attacks and man-in-the-middle attacks. However, when the challenge values are disclosed, it is susceptible to communication attacks (Gong *et al.*, 2013; Chow *et al.*, 2015; Son *et al.*, 2019).

2.1.4 S/Key authentication. This authentication is also known as the Lamport scheme and in this scheme, OTP values are generated using hash chaining from the secret key (N. Haller, 1995). In this process of OTP-based authentication client and server, after sharing a

secret key generates hash value, the generated hash value is taken as input by the second hash function. N times, the algorithm repeats this procedure. If we consider the one-way hash function as f, the secret key S and apply f to the seed S for N times, we get a hash chain of length N:

$$f(S), f\left(f(S)\right), \ldots, fN(S) \tag{1}$$

On the client-side, N hash values are stored and on the server-side, f (S), f (f (S)) . . .. f^{N-1} (S) are discarded and only f^{N} (S) is only stored. When the client is authenticated, the N−1 hash is sent to the server by the client. The server generates the *N-th* hash value from the N−1 hash of the client and compares it with the *N-th* hash value, which is already stored to check whether the user is legitimate. At the user *m-th* login, the server sends challenge code (N-m) and the user generates the OTP as follows:

$$OTP = f^{N-m}(s) \tag{2}$$

The server authenticates the user's OTP as:

$$\mathrm{f}(\mathrm{OTP}) = f^{\mathrm{N-m+1}}(\mathrm{S}) \tag{3}$$

The f^{N-m+1} (S) is already memorized in the server after the $(m-1)^{th}$ login. If the client and server's above values are the same, the server stores the received hash value and deletes the previous $(N-(m-1)^{th}$ hash value. This scheme is straightforward to implement, combines both challenge and hash chaining and does not need exceptional hardware support (Li *et al.*, 2010; *S/KEY-Wikipedia*, 2020). The S/Key authentication is vulnerable if an attacker impersonating the host sends a small challenge to the user, who responds with the hash chain's initial values, allowing the attacker to compute more OTPs. This type of attack is known as a "small challenge" attack. Furthermore, the user's computing requirements are higher during the computations for the chain's initial values, rendering the system infeasible for limited resource devices such as cell phones. Despite being impervious to eavesdropping and replay attacks, the scheme is vulnerable to server-spoofing and offline dictionary attacks (Eldefrawy *et al.*, 2010).

2.1.5 Short message service-based one-time passwords. The advancement in smartphone technologies utilization of self-care services in banking, health care and e-commerce has increased significantly. Providing security in terms of authenticating and authorizing legitimate users is the biggest challenge the organizations face in rolling out these services. Traditional ways of authenticating users based on knowledge factors such as usernames and passwords have serious issues being compromised by intruders. These mechanisms are susceptible to various kinds of attacks such as password guessing attacks, shoulder surfing attacks and brute force attacks (Kuo and Lee, 2007; Towhidi *et al.*, 2011; Komanduri *et al.*, 2019). OTP was implemented as an additional factor to gain access only to the authorized users to counter such attacks. The rudimentary idea of a one-time password is that every client account is bound to a cell phone number in a system in control of the proprietor of the account.

Consequently, the account's proprietor is the solitary individual who can get the short message service (SMS) OTP ship off the versatile number connected to the account. In this authentication process, clients are needed to enter a one-time password in the wake of giving a username and secret phrase to approve the transaction; each produced OTP is used once and afterward disposed off. The appropriate way of sending one-time passwords generated

by the authenticator is through an SMS, which avoids creating password lists (Babkin and Epishkina, 2019). Most banks and other organizations providing online services such as Google Mail, Dropbox, Google App Engine use SMS-based OTP for account verification. SMS-based OTP is considered safe because every time the user has to enter newly generated passwords, it is secure from temporary exposure and strengths the system against reply attacks (Huang *et al.*, 2013).

2.2 Biometrics-based authentication

Authentication systems based on knowledge and physical token are generally accepted due to ease of implementation, design simplicity and familiarity, although used in several modern applications, cannot meet strict security performance requirements. One good alternative to this authentication system is Biometric-Based-Authentication that uses a user's unique physiological or behavioral characteristics for identification and authentication, such as the face, fingerprint, hand geometry, iris, keystroke, signatures and speech (Biometrics-Home, 2021; Bolle *et al.*, 2004). The user's traits for authentication are bound with the individual much more profound level than knowledge and token-based authentication. Consequently, they are inherently more reliable because biometric features cannot be misplaced or overlooked; they are exceedingly hard to duplicate, share or exchange and they enable the individual to be available at the moment of authentication. As per the information provided by the International Biometrics Group, There is no one right biometrics technology for every application (Bowler, 2006). The following are some of the most widely used biometrics in today's automatic authentication systems:

2.2.1 Fingerprint. For a long time, the fingerprint is being used as a distinctive and accurate identification of suspects, resolve crimes and remains a valuable tool for law enforcement and other government organizations. When tested, fingerprints have proved to have the highest security degree, with no attempts to deceive the system reported. While certain variables can trigger false positives and negatives, such as dirt, makeup and age, the error rate is 1 in 500 or higher, rendering this function superior to other biometrics.

2.2.2 Retinal or iris scan. This biometric identify a person by analyzing the arrangement of veins in the retina or the color patterns in the iris. Iris scans have been effectively used for user authentication but are not devoid of issues, e.g. glasses and inappropriate lighting can result in a false reading. Iris scans are generally not very difficult to fool but have an acceptance rate of about 1–131,000, which is relatively good. Retinal scanners show an improvement over iris scanners to authenticate even blind users or users lacking iris pigment. Moreover, retinal scans are difficult to be fooled with a particular error rate of 1 in 1,000,000, which is extraordinary among all other biometric features:

- Voice recognition: It makes use of a voiceprint examining how an individual utters a word or a word sequence exclusive to him. An attacker may capture the authenticated user's voice and use it to bypass the voice recognition authentication system.
- Facial recognition: A person can be identified through his unique facial attributes. However, such authentication systems can be fooled through a mask at the default setting, which increasing threshold levels can overcome to 96%. Furthermore, the facial features may not remain the same with age.

An added advantage of biometric usage in authentication is the low cost incurred by fingerprint technology that costs around US$100.00. On the other hand, retina scans costing US$2,000.00–US$2,500.00 put the technology at the end of the cost scale. Nonetheless, it provides high reliability that cannot be compromised in areas demanding extraordinary

security (OS Timeline, 2020). The effectiveness of any biometric application is determined by combining all these attributes. There is neither biometric that satisfies any of the attributes absolutely nor one which has all to completely acceptable level simultaneously, resulting in many compromises (Joshi *et al.*, 2018). Biometric authentication systems, although providing essential usability advantages like other systems, are susceptible to many threats. Biometrics captures features such as blood vessel shapes, retina, pulse rhythms; unlike knowledge-based authentication mechanisms that can be quickly reset if the device is corrupted, it is challenging to reset biometric-based authentication systems.

Moreover, biometric-authentication is not very responsive to the changes; small changes in facial expression, obstruction due to glasses, scarves and hats can deny access to confidential data even to the right individuals (Uludag and Jain, 2004). Biometric authentication methods have broadly expanded in recent years due to the demand for suitable authentication methods increased. With the incorporation of state-of-the-art scanners in numerous gadgets and other biometric strategies coming into more extensive use, it is apparent that biometric authentication is used as a secure and cost-effective authentication mechanism future (Vic Berger, 2007). As biometric traits authenticate the user in the best possible way to add on the security, it should not be used as a stand-alone form of authentication. Be that as it may, biometrics can be used as a feature of secure, two-factor or MFA when joined with other validation factors as a second or third confirmation factor. This methodology defeats many security drawbacks while providing an advantageous user experience (Abhishek *et al.*, 2013).

2.3 Multi-factor authentication

To prevent an adversary from accessing critical and sensitive information, MFA is one of the most effective controls organizations may use. More than one authentication factor is chosen from independent categories of credentials to identify legitimate users (Ba and Ren, 2017). The factors selected for identifying legitimate users in MFA should be autonomous of each other with the end goal that accesses to one factor does not concede access to some other factor and the tradeoff of any one factor does not influence the respectability or secrecy of some other factor. MFA is the layered approach for securing sensitive information and applications. The system requires users to present two or more authentication factors to identify the legitimate user in this type of authentication. A famous example of MFA is commonly used in bank ATMs to complete any financial transactions in which something the user possesses, that is, an ATM card combined with something the user knows PIN is used to identify the legitimate bank user. The customer must carry both debit or credit cards and provide a personal identification number while using ATM services. If someone steals or finds a lost card has to know or guess the customer's pin, which constitutes better security than a password alone. The advantages of MFA are that intruders need to move beyond not one but rather many authentication devices. When implemented effectively, such authentication devices would need to fizzle in various manners before security is seriously compromised (Sanyal *et al.*, 2010; Ometov and Bezzateev, 2017; Ometov *et al.*, 2018). The undeniable advantage of MFA has expanded security by adding extra layers of assurance. The more layers (factors), the harder it is for a possible intruder to access records, frameworks or information. MFA can likewise assist organizations with accomplishing and look after consistency, which can decrease possible legitimate obligations. Due to the adaptation of smartphones and other widgets and incorporation of integrated biometric interfaces, for the most part, MFA is based on biometrics, which contributes significantly by improving identity proofing by adding knowledge factor with biometrics factor to provide an additional level of security, thus making it difficult for intruders to penetrate a system

(Sabzevar and Stavrou, 2008; Sanyal *et al.*, 2010; Deborah Golden, 2015; Development, 2016). Without question, biometrics is one of the most critical levels for potential authentication. The anticipated progression toward MFA is embedded in synergistic biometric systems that dramatically increase user experience and throughput, which is helpful in several applications. These systems can consider these three factors as follows: what you know, what you have and what you are.

3. Open issues and challenges

After conducting the review of previous research works, the open issues explored from security, access management and adaptability perspective have been given below as follows:

- SMS-based OTP's security is dependent on the privacy of the cellular network. Serval attacks against GSM and 3G have been reported, which has shown that secrecy of SMS messages cannot be provided. Privacy of SMS can also be compromised by injecting malware in mobile phones, which can intercept and forward OTP SMS to attackers, thus making it vulnerable to man-in-middle attacks. SIM Swap attack is one more attack against SMS-based OTP, a social engineering attack in which SIM card replacement for victims' mobile numbers is acquired. The SIM card is then linked to the mobile number of victims; thus all OTP SMS is then received by the attacker while initiating online transactions (Paper *et al.*, 2013; Yoo, Kang and Kim, 2015; Gilsenan, 2018; Suker, 2019; Kim *et al.*, 2020).
- As users travel outside of the coverage area for SMS-based two-factor authentication, they face the inconvenience they face accessing incoming SMS containing OTP (Mehraj *et al.*, 2015).
- The analysis shows that a more significant part of the OTP computation procedures depends on time synchronization, numerical calculations to generate one-time passwords. The arbitrariness of these OTP frameworks breaks after a timeframe and consequently, passwords become foreseeable (Choi and Kwon, 2015; Lone and Mir, 2019).
- Weak password generation methods, such as MD5, AES, SHA-1 and others, are used in most authentication schemes (Alzomai, 2010; Deore and Waghmare, 2016), leaving them vulnerable and struggling to help on time owing to technical advances. When used on a public network, SHA-1 poses various problems, so it cannot be selected (or modified) by an investigator when performing experiments in broad public networks with a high degree of unguided intrusion cases.
- Some authentication systems necessitate additional equipment (Wang and Chang, 1996; Hsieh and Leu, 2011) like smartcards cause inconvenience to the users and demonstrate exorbitant to specialist co-op. Accordingly, these authentication mechanisms are not feasible to implement. In this manner, the specialized adaptability of these frameworks is being hampered because they need ease of use.
- Contemporary schemes (Aboud, 2014; Xiaoyi Duan, 2016) have been found to have several issues, including increased processing time, computing expense, decreased device speed and broad storage due to fuzzy vault schemes, public key operations and self-updating hash chains.
- The integration of biometric for effective user authentication inside a cryptographic framework bodes well; there are various difficulties associated with integrating biometrics in cryptosystems, principally because of the dramatic variation in the

representation of biometric identifiers and because of a depraved idea of biometric feature extraction and matching algorithm. Also, using biometrics for user authentication using cell phones stays a mind complex procedure because of equipment constraints, noisy and inconsistent data and adversarial attacks (Uludag *et al.*, 2004).

- The current authentication schemes depend on a single biometric trait as the third authentication factor or in certain situations, just biometrics, missing the first two authentication factors, may be susceptible to impersonation attacks. Consequently, such authentication mechanisms have security flaws and cannot be used in applications that need high security, such as banking and airport information systems (Moon *et al.*, 2012; Avhad and Satyanarayana, 2014; Oruh, 2021).

4. Proposed authentication scheme

Recent advancements in mobile phone technology, especially in storage and cognitive capability, have been increasingly exploited for remote access to services like e-commerce and online banking transactions (Jang-Jaccard and Nepal, 2014). Access to these services from mobile phones has led to an increased demand for more digital identification by providing adequate security solutions for user authentication. Traditional authentication mechanisms that use knowledge and a physical token cannot meet the requirements for adaptation effective security solutions because of security issues. Identification of users based on biometric features can replace conventional authentication techniques because of the incorporation of low-cost advanced sensing platforms in mobile phones, which opens an emerging frontier for trustworthy authentications for accessing remote services in internet applications, mobile bank transactions and telemedicine monitoring (Licenses, 2020). Despite the advantages of biometric authentication, there are many unsolved issues associated with this sort of authentication mechanism; designing an appropriate authentication mechanism that is accurate, reliable, cost-effective, user-friendly and can be used without severe changes to existing infrastructure is anticipated. In this section, a novel OTP-based tripartite authentication scheme is proposed which takes into account all the three factors of authentication to achieve higher security while authenticating legitimate users and at the same time overcomes the limitations in existing authentication mechanisms addressed in the current study.

4.1 Design of novel one-time password-based tripartite authentication scheme

This paper aims to design an authentication scheme that authenticates legitimate users in a more secure and user-friendly manner in mobile applications used to access critical information. The main idea of the proposed authentication scheme is to develop a challenge-response authentication mechanism in which all the three authentication factors that knowledge (username), token (Device Number) and possession (Fingerprint) are used as a secret key between client and server before authentication. The current scheme adopts application-based authentication, thereby guarantees data confidentiality and improved security; as in the challenge-response authentication mechanism, the server sends challenge values each time differently to the client to generate a one-time password. The overall procedure of the proposed OTP-based tripartite authentication is shown in Figure 1. The algorithm progress as follows:

- The user registers username, device number and fingerprint with the server through a mobile application, which is used as a secret key.

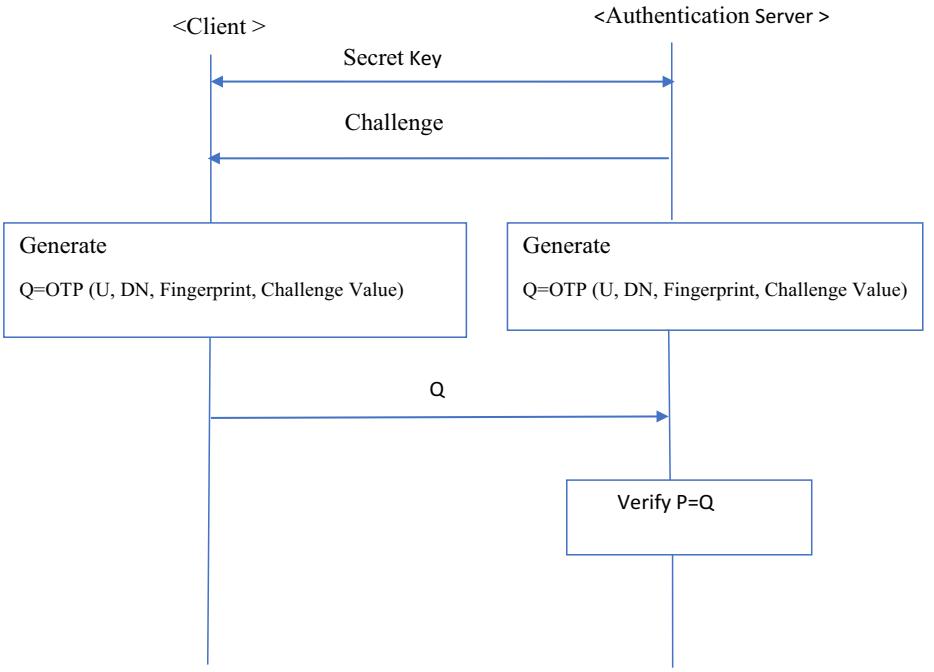

Figure 1. Proposed authentication scheme

- When the server is requested to authenticate the client, the server sends a challenge value to the client.
- The client provides its username, device number and scans fingerprint; OTP is generated using these three factors by the client and is sent to the server.
- 4. The server generates an OTP value with already registered user factors using the same algorithm as the client.
- The server compares its OTP value with the one received from the client; if both matches user is considered a legitimate user; otherwise, not.

4.2 One-time password generation algorithm

For granting access to confidential and sensitive information on the internet, validating and verifying legitimate users is an elementary step. Out of the various authentication mechanisms developed for security, SMS-based OTP is generally used as an additional factor for secure authentication. In this authentication mechanism in a system, each account is linked with a mobile phone in the account owner's possession. The SMS-based OTP provides a pathway for double layer security, which requires a validation of user credentials that are username and password followed by generation of one-time password sent to the mobile phone linked to the user account. OTP's are random numbers that are generated uniquely for each authentication event. Thus, the one-time password is an additional factor of security in web-based services generated each time authentication is attempted by the user to access a resource and is unpredictable for the next session making SMS a substantial part of the MFA and/authorization applications. According to the current study, most OTP

generation mechanisms are centered around time-synchronization, mathematical algorithms and other related mechanisms to produce a one-time password. The OTP arbitrariness of these frameworks break after some time; thus the password becomes predictable.

Most of these services still use SMS-based OTP, which is no longer considered secure as per the National Institute of Standards and Technology (NIST) issued in 2016(Grassi *et al.*, 2017). Moreover, the use of hash functions, such as SHA1, other hash functions from the MD family-like MD5, are used in specific OTP computational mechanisms that are not, at this point, thought secure cryptography. Instead of the error-prone and traditional SHA-1, the analysis uses RIPEMD16 for OTP generation. Biometrics-based authentication frameworks are now a day turning out to be a convention of anticipation for unauthorized access, fraud and different sorts of attacks. Users are validated and approved using these methods based on their unique physiological/behavioral characteristics (Jain and Bolle, 1999), which are novel and sensibly lasting and do not change. In addition to the standard usage of passwords, tokens/smartcards or a hybrid of the two, integrating biometrics as a degree of security coupled with two-factor or MFA would undoubtedly increase the reliability of the authentication process.

To overcome the shortcomings discussed above, this research proposes a mechanism for generating one-time passwords in OTP clients and servers that combines all three authentication factors as follows: something you know, something you have and something you are. In the proposed password creation method, the username, the user's device number and fingerprint features are used as a seed for OTP generation. One of the significant enhancements performed in the proposed method is the inclusion of fingerprint features in OTP generation to ensure higher security. The whole procedure of password creation is given in Figure 2 – the complete algorithm for OTP generation progress as follows:

- The user or client registers with the authentication server credentials username, device number and fingerprints, used as the initial seed for OTP generation through the mobile application.
- While authenticating the user, the username, device number and live fingerprint are taken from the user.
- The OTP module extracts the features of the fingerprint converts fingerprint features into a unique string. The complete feature extraction process and conversion of features into a unique string are described in Section 4.3.
- The username, device number and string generated from fingerprint features are concatenated to form the seed for OTP generation.
- The seed generated in Step 4 is input to RIPMED160 for a hash generation; the 160-bit hash is generated at this step. The RIPEMD 160 is chained N times where N is the challenge value send by the server. The use of RIPEMD 160 would have two distinct benefits as follows: A hash of 160 bits provides more security. TOTP previously standardized a Dynamic Truncation method for generating 6-digit OTP numbers using 160-bit hash values. While SHA1 is the most well-known hash algorithm for 160-bit hashes, it is vulnerable to attacks on a theoretical basis. As a consequence, RIPEMD 160 emerges as a superior choice.
- 160-bit hash generated by the RIPEMD160 is truncated to convert this 160-bit hash into a 4-byte string.
- The 4-byte string is converted into a 6- or 8-digits user-friendly OTP.

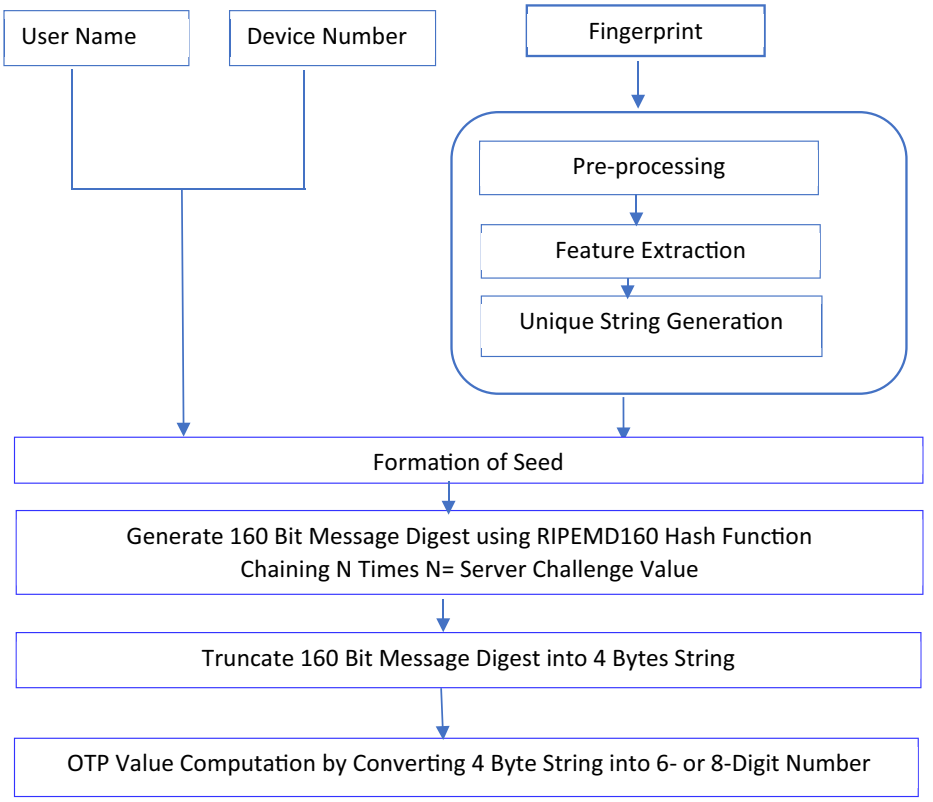

Figure 2.
Proposed OTP generation process

4.3 Generation of unique string from fingerprint features

Fingerprints are the most well-known biometric characteristic for identifying individuals. For more than 10 decades, it is being used to identify suspects, resolve crimes; it remains a valuable tool for law enforcement because of its reliability and security. Due to the integration of fingerprint sensing frameworks in smartphones, personal computers and tabs, fingerprint sensing is increasingly common, convenient for user authentication for accessing critical services. Compared to other biometric characteristics (such as the face, iris and voice), fingerprint-based identification systems have been extensively tested, with no reported attempts to deceive. The accuracy of the identity authentication system, based on fingerprints, has been stated to be very high. While some situations, such as dirt, makeup and age, can cause false positives error and false negatives errors, an error rate of 1 in 500 or higher has been discovered, making the fingerprint feature more effective than other biometric traits (Jain *et al.*, 2007).

A fingerprint is a distinctive pattern of valleys and ridges on an individual's finger surface. The ridge is an elevated part of the epidermis that persists throughout a person's life on the finger. The region between two head-to-head ridges is known as a valley. Ridges and valleys sometimes run parallel to one another, bifurcating and terminating at times. Fingerprints are divided into the following major groups shown in Figure 3 based on the fingerprint pattern of ridge formation.

The most prominent structural features on the fingerprint surface called minutia used to differentiate two fingerprints may be determined without difficulties. Among about 150 different types of minutia, ridge ending and ridge bifurcation are most commonly used. All other minutiae can be seen as a combination of these two. The core and delta points, also known as singular points, are two critical locations of the fingerprint usually characterized by areas of high curvature where ridge abruptly changes used to classify fingerprint images to reduce the search space. These points are the high-level most important fingerprint features and are highly stable and rotation and scale-invariant. Singular points such as core are the most accurate and they are found in the majority of fingerprints. It is the maximum curvature in the fingerprint ridge and the topmost point of the innermost ridgelines. The core point is a particular point in a fingerprint that can be used as a starting point for calculating other minutia points (Kumar, 2020; Zabala-Blanco *et al.*, 2020). By observing and comparing the minutia characteristics of two different fingerprints that occupy the same relative area and location, they can be distinguished from one another. The study proposes several methods for detecting singular points using an orientation field image. In the proposed analysis, Poincare Index Method is used, a common and realistic method for recognizing these points from a fingerprint (Magalhães *et al.*, 2009; Li *et al.*, 2013; Iwasokun and Akinyokun, 2014; Lone and Mir, 2019). An input image of the fingerprint must first be converted into an orientation field before the Poincare Index Method can be applied to it. The Poincare index of all the points in the orientation image is computed by adding the field angle differences of consecutive points and the point enclosed by a digital curve (Core Point) has the highest Poincare index. We consider the scenario where eight positions are taken around a particular 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 $\theta\ (i, j)$ be the (i, j) – element of an orientation field image and $0 \leq \theta\ (i, j) < 2\pi$ for any (i, j) Let:

$$\delta k(i, j) \ = \ \theta\ (i_{k+1}, j_{k+1}) \ - \ \theta\ (i_k, j_k) \tag{1}$$

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:*

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

where,

Figure 3.
Fingerprint patterns

$$\Delta_{\mathrm{k}}(\mathrm{i},\mathrm{j}) = \begin{cases} \delta_{\mathrm{k}}(\mathrm{i},\mathrm{j})\, if \mid \delta_{\mathrm{k}}(i,j)\mid < \pi/2 \\ \pi + \delta_{\mathrm{k}}(\mathrm{i},\mathrm{j})\, if \;\; \delta_{\mathrm{k}}(i,j) \leq -\pi/2 \\ \pi - \delta_{\mathrm{k}}(i,j)\, otherwise \end{cases} \tag{3}$$

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.

Once the core point has been determined, other details such as ridge ending and ridge bifurcation can be quickly traced using the core point as a point of reference. The input image quality must be improved by applying pre-processing filters such as two-dimensional (2D) median and 2D adaptive wiener filters, which improve image quality by removing noise and obtaining the other minutia's points efficiently and consistently. After enhancing the image's quality in pre-processing step, the minutia extraction begins by converting it to a binarized image, which entails converting a pixel value to 1 if it is greater than the mean intensity value of the current block to which the pixel belongs. Thinning, also known as skeletonization, which reduces the width of all ridgelines to a single pixel, is another significant pre-processing procedure used on the image after binarization displays the fingerprint ridge pattern as a single line skeletal view. After thinning the fingerprint ridges, the next step is to marking minutia points. The probability of an accurate result rises as the number of minutiae detected is more. For extracting minutiae, the principle of Crossing Number (C.N.) is commonly used. For a pixel, the P, C.N. is specified by Rutovitz as equation (4):

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

P_i = (0 or 1) and P1 = P9, Pi is the binary pixel value in the neighborhood of P. The C.N. Cn (P) of a particular point P is equivalent to half of the cumulative number of successive differences between pairs of neighboring pixels in P's eight neighborhood. A ridge pixel may be classified as an ending, bifurcation or non-minutia point using the C.N. properties.

If Cn(P) = = 1 it is a ridge end and if Cn(P) = = 3 it is a ridge bifurcation. As more emphasis is given on ridge ends and ridge bifurcations, this is the best situation and there is no need to consider Cn(P) > 3 as it is a crossing point. After minutia marking, the image must go through a minutia post-processing phase because the earlier stages would have added much spurious minutia. The following are the various methods used to remove spurious minutia from images:

- If the distance between one bifurcation and one termination is less than D and the two minutiae are in the same ridge. Both of them should be removed.
- If the distance between two bifurcations is less than D and they are in the same ridge, remove the concerned minutia that appears to be two bifurcations.
- Minutiae are removed if the distance between two terminations is less than D.

Where D is the Euclidean Distance, which is six pixels in this study.

There would still be many specific minutiae needed to generate the unique string after removing the spurious minutia from the image. Minutia points centered around the core point are only considered for the generation of unique strings. The image now just has the absolute minimum of minutia marks. The *x*- and *y*-axes coordinates and the orientation angle relative to the origin define the minutia points' location around the central point in the fingerprint. As a result, the minutia points are reshaped into an NX3 matrix containing minutia x, y and orientation angles. This matrix is then transformed into a unique string.

5. Experimental results and discussion

To evaluate the performance, advantages and disadvantages of the proposed novel OTP-based tripartite authentication scheme, a client-server-based working prototype was developed. The client application was developed using android and the server-side application using java. The client application can run on any smartphone with an android operating system. The client application that needs to be installed on the client-side in the smartphone has two modules as follows: registration and user verification. In the registration module, users have to enter their username and scan their fingerprints; the device number is read by the registration programming module and stored on the server in a database. When the user has to be authenticated for granting access to critical information, the user provides all his credentials: the username; Device number is automatically read and the live fingerprint, the algorithm for generating OTP as discussed is implemented using android to generate OTP in the verification module. The server-side programming module for generating OTP from the credentials registered by the user is hosted on a web server; for the current experiment, Firebase has been used to host both server-side programs and the database. A database is needed on the server-side to store user credentials such as username, device number and fingerprint features. For generating OTP on the server-side, the server-side program takes particular user credentials from the database and uses the proposed OTP generation algorithm to generate an OTP.

Experiments to evaluate the performance of the proposed novel OTP-based tripartite authentication system were conducted in a controlled lab environment in which users from different educational backgrounds and ages participated. The experiment involved 35 participants, including university students, teaching and non-teaching staff familiar with smartphone applications. The percipients were given hands-on training to install the client application for registration and verification of the user and overall know how to use the proposed authentication scheme on smartphones. For evaluating the performance of the proposed protocol after registration, each participant was evaluated for authentication by each user was allowed a maximum of five attempts for authentication. The following performance evaluation metrics were used to evaluate the performance of the proposed authentication protocol.

5.1 Failure to enroll

Most importantly, all authentic users must be enrolled. At this level, issues occur because of specific reasons some users cannot be enrolled. So, failure to enroll (FTE) is the percentage of genuine users that cannot be enrolled or registered.

$$\text{Failure to Enroll (FTE)} = \text{Number of Failed Enrollment} / \text{All Genuine Enrollment Attempts}$$

One out of the 35 participants could not register because the fingerprint sensor could not produce an image of sufficient quality to enroll fingerprint. In this, several attempts were allowed to achieve an enrolment. The FTE Rate of the proposed system is given in the following graph in Figure 4. The FTE Rate for the proposed system is 0.02.

5.2 True acceptance rate

The true acceptance rate (TAR) is the statistics used to measure the performance when verifying the legitimate user by the biometric system. It is the ratio of the number of times the biometric system correctly checks a genuine user.

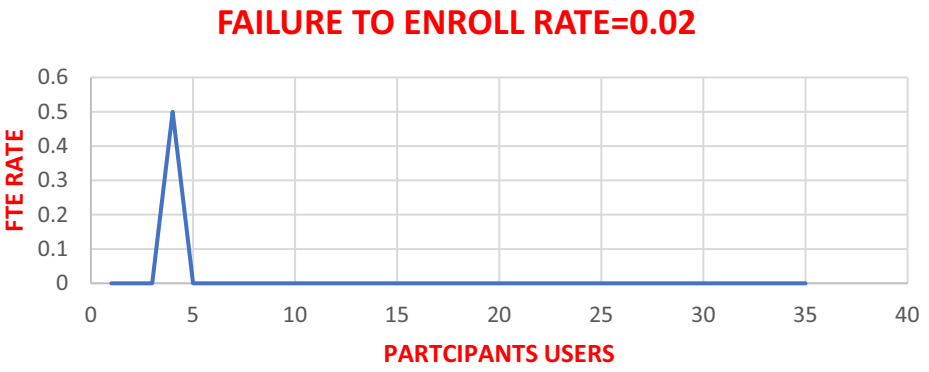

Figure 4.
FTE rate

True Acceptance Rate (TAR) = Number of True acceptances/Number of genuine user attempts

For calculating the TAR, each registered user was allowed to authenticate himself using the proposed authentication scheme five times at different intervals of time. The TAR of the authentication scheme was calculated at a threshold of 75%. The TAR graph given in Figure 5 shows the value of the TAR achieved is high, 98.28.

5.3 False rejection rate

A false rejection occurs when the biometric system rejects the legitimate user as an illegitimate one. The false rejection rate (FRR) is calculated as the ratio of the number of false rejections to the total number of genuine user attempts.

False Rejection Rate (FRR) = Number of False rejection/Number of genuine user attempts

The proposed authentication scheme can be seen in the graph below that FRR is 1.71, which is very low (Figure 6).

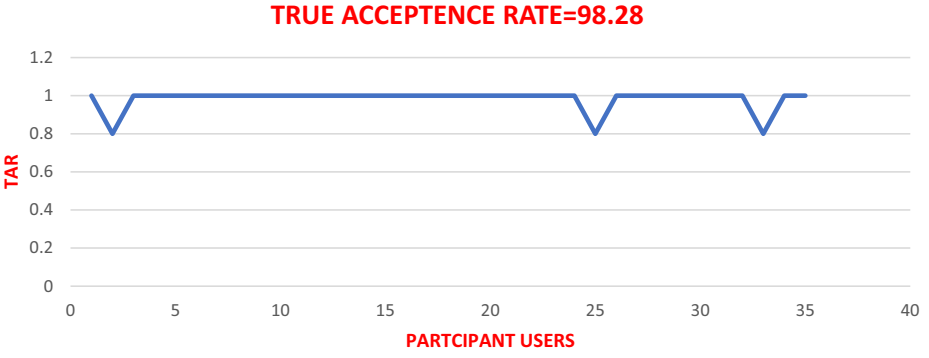

Figure 5.
TAR

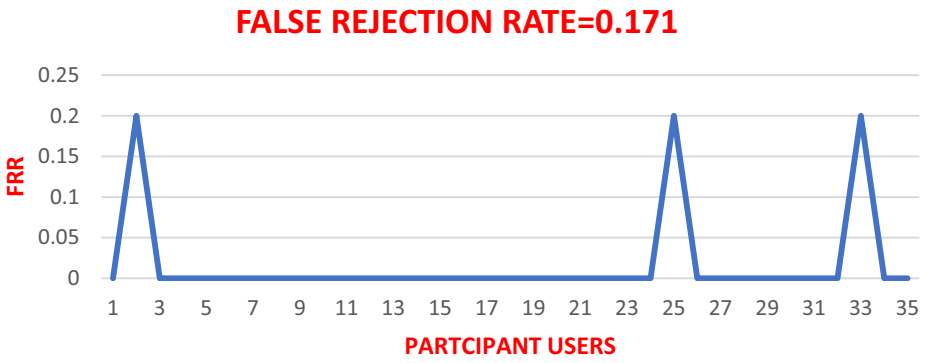

Figure 6.
FRR

5.4 True rejection rate

The true rejection rate (TRR) is the measure used to calculate the performance of a biometric system when authenticating legitimate users. It refers to the percentage of times an illegitimate user has been correctly rejected by the biometric system and calculated below:

$$\text{True Rejection Rate (TRR)} = \text{Number of false Rejections/Number of Imposter attempts.}$$

For the proposed authentication scheme, 35 users already registered were asked to authenticate themselves in the five attempts with the finger not registered already to act as an imposter. For performance evaluation, registered users are allowed to register only one fingerprint in the proposed authentication scheme. The TRR rate of the proposed system is given in Figure 7, calculated on a 75% threshold value. From the TRR, it can be seen that the TRR value is 98.85, which is considered very high.

5.5 False acceptance rate

The false acceptance rate (FAR) is one of the key performance metrics for measuring the performance of biometric systems. It is the percentage of identification instances in which the biometric system incorrectly accepts illegitimate users.

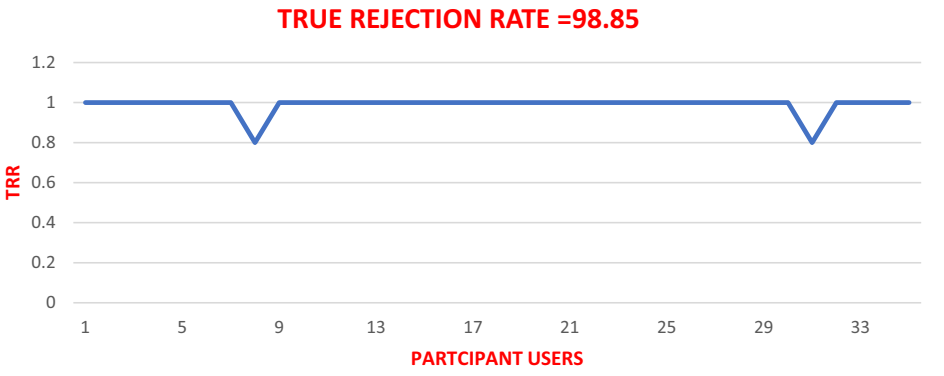

Figure 7.
TRR

False Acceptance Rate (FAR) = number of false acceptance/number of impostor attempts.

In the proposed authentication scheme same process has been used for calculating TRR. All the registered users have tried to log in with the fingerprint not registered with the biometric system. The average attempts counted for calculating FAR was five for each user on a threshold of 75%. The input fingerprint at the time of verification was compared with the fingerprint template stored on the server and FAR was calculated as shown in Figure 8 as 0.017, which is considered low.

6. Usability evaluation of proposed authentication scheme

Due to increasing deployments and affordable hardware components in smartphones and personal gadgets, the advent of biometrics as a means of authentication has accelerated in govt organizations, financial institutions and health care. The incorporation of biometrics in MFA schemes should be convenient to the user, easy to learn and impel to use. As the proposed authentication scheme uses all three authentication factors to authenticate a legitimate user, it is essential to see how effective this authentication scheme is in terms of its usability. The primary intention of the usability evaluation of the proposed authentication is to obtain a usability conclusion for future developments. For evaluating the usability of the proposed scheme, measures from previous studies ISO-9241–11 were extracted. As per this standard, effectiveness, efficiency and satisfaction are the main components of usability in a particular context (Lashkari and Farmand, 2009; Kainda, Flechais and Roscoe, 2010; Gunson *et al.*, 2011; Ali, 2013; *ISO-ISO 9241–11*, 2018; Acemyan *et al.*, 2018; Reese, 2018; For and Release, 2019; Oh, Lee and Lee, 2019). The experiment to conduct the usability evaluation of the proposed authentication was conducted in a controlled lab environment where the mobile application developed for the proposed authentication was installed on mobile phones. The first session overview of the proposed authentication scheme and explanation of its functionalities enrollment and authentication was given. All the users, after successfully getting registered, their authentication factors username, device number and fingerprint were asked to authenticate through the verification module. The mobile application generated some significant activity logs that store registration and verification time for each user to calculate the efficiency and effectiveness. The experiment was conducted in five different trials and in each trial, users were instructed to authenticate themselves using a verification module. After completion of the five trials, qualitative results for efficiency and effectiveness were calculated.

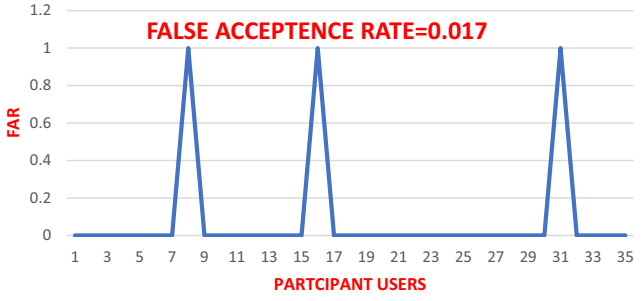

Figure 8.
FAR

6.1 Efficiency

While users may use a framework to accomplish an explicit objective, accomplishment in itself is not adequate. The objective should be accomplished inside a good measure of time and exertion. Efficiency is captured by measuring the time to complete a task. For the proposed authentication scheme, efficiency for registration and verification/authentication was calculated using the following (Table 1):

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

From the results, it is clearly shown that for registration and verification of users in the proposed scheme, it took 15 s and 18 s, which indicates how efficiently and quickly the proposed scheme can be used for authentication.

6.2 Effectiveness

Effectiveness has a significant influence on the satisfaction factor and, according to ISO-9241, is defined as the accuracy and completeness with which the user archives specified goals. In the proposed scheme, the effectiveness has been calculated as a total number of successful logins across all the login attempts while authenticating a legitimate user. For the current scheme total number of 35 users are registered and five attempts from each user have been considered to calculate the effectiveness. The login success rate is calculated as follows (Table 2):

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

From the results, the study shows that the successful login rate is very high; 98.28% of registered users were able to authenticate themselves without any error successfully and 1.71% failed to login because of the error in the fingerprint scanned by the mobile application could not match with the stored template of the fingerprint on the server. Hence, OTP generated on client and server could not match.

Table 1. Efficiency of proposed authentication scheme

	Total attempts	Total time	Average	SD	Minimum	Maximum
Registration	35	552	15	3.68	13	30
Verification/authentication	35	648	18	4.41	13	28

Table 2. Effectiveness of proposed authentication scheme

Total attempts	Successful		Failed	
175	172	98.28%	3	1.71%

6.3 User satisfaction

After completing all attempts to authenticate the registered users, all the 35 users were given questionnaires to see their feelings toward apparent usability features. In contrast to Efficiency and Effectiveness, user satisfaction aims at the subjective thoughts of the user and describes the comfort and relevance of the application. For the proposed scheme system usability scale (SUS) was used to measure the user satisfaction of the users (Brooke, 1996; Jeff Sauro, 2011; Thomas, 2020). SUS is a Likert 10-item scale based on forced-choice questions giving a global view of the subjective view of usability assessment. It is generally used after the user has an opportunity to use the system being evaluated. SUS score tells your usability performance in effectiveness, efficiency and overall ease of use and ranges from 0–100. The average SUS score is 68. The SUS score was calculated based on users' responses in the questionnaire; both individual and overall SUS score was calculated as given in the graph below (Figure 9).

The proposed authentication scheme SUS score of 74.4 has been achieved, which comes under a good adjective rating.

7. Conclusion

Mobile devices are unquestionably the way of the future and they are now ubiquitous in our everyday lives for accessing remote services such as e-commerce and online banking transactions. The integration of low-cost advanced sensing platforms for biometrics in mobile phones has made it easy for users to provide biometric traits in MFA, thus simplifying the development of secure and reliable authentication schemes. The authenticated scheme presented in this paper is based on challenge-response-based authentication in which all the three authentication factors are something you know (knowledge), something you have (possession) and something you are (inherence) to generate a one-time-password. The proposed scheme has been developed for smartphones in which username, device number and fingerprint features are used to generate an OTP. Using all these authentication factors makes it resistant to Man-in-Middle attacks, password guessing, replay attack and complements vulnerabilities such as MITPhone, SIM Swap attack and SMS-based OTP authentication.

Furthermore, as most general mechanisms for generating OTPs are centered on synchronization of time of client and server and mathematical algorithms, the arbitrariness of these OTP systems breaks after some period, thus making passwords predictable. As a result, a safe and user-friendly OTP computational process is required and one such method has been proposed in the current study. The model generates OTP using the user's information (username), possession (device number) and inherence (fingerprint) factors as the initial seed, making it difficult for the attacker to predict the output and thus secure from guessing attacks. The proposed model also meets the criteria of digital authentication guidelines 2016 by NIST, which acknowledges that biometrics as a means of authentication shall be used with another authentication factor ("something you know" or "something you

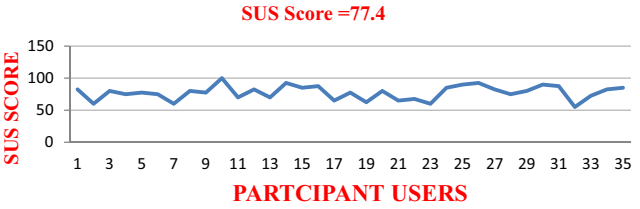

Figure 9.
SUS score

have"). The initial results of performance and usability testing of the proposed authentication scheme show that current authentication has a high degree of efficiency, effectiveness and user satisfaction. It can succeed and lead to MFA adaptation.

References

Jain, A.K. and Bolle, S.P. (1999), "Biometrics: Personal identification in networked security, personal identification in networked society".

Abhishek, K., *et al.* (2013), "A comprehensive study on multifactor authentication schemes", *In Advances in Intelligent Systems and Computing*, pp. 561-568, doi: 10.1007/978-3-642-31552-7_57.

Aboud, S.J. (2014), "Secure password authentication system uisng smart card", *International Journal of Emerging Trends and Technology in Computer Science (IJETTCS)*, Vol. 3, pp. 75-79.

Acemyan, C.Z., *et al.* (2018), "2FA might be secure, but it's not usable: a summative usability assessment of google's two-factor authentication (2FA) methods", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 62 No. 1, pp. 1141-1145, doi: 10.1177/1541931218621262.

Ali, A. (2013), "[THESIS] a framework for measuring the usability issues and criteria of mobile learning applications".

Alzomai, M. (2010), "The mobile phone as a multi OTP", *in 2010 Fourth International Conference on Network and System Security*, pp. 75-82, doi: 10.1109/NSS.2010.39.

Avhad, P.R. and Satyanarayana, R. (2014), "A Three-Factor authentication scheme in ATM", *International Journal of Science and Research (IJSR)*, Vol. 3 No. 4, pp. 2-5.

Ba, Z. and Ren, K. (2017), "Addressing Smartphone-Based multi-factor authentication via Hardware-Rooted technologies", *in Proceedings – International Conference on Distributed Computing Systems*, doi: 10.1109/ICDCS.2017.88.

Babkin, S. and Epishkina, A. (2019), "Authentication protocols based on One-Time passwords", pp. 1794-1798.

Beikverdi, A. and Tan, I.K.T. (2012), "improved look-ahead re-synchronization window for hmac-based one-time password", *in IET International Conference on Wireless Communications and Applications (ICWCA 2012)*, pp. 1-5.

Biometrics - Home (2021), available at: https://biometricstoday.weebly.com/ (accessed 25 October 2020).

Bolle, R.M. *et al.* (2004), "Guide to biometrics, guide to biometrics", doi: 10.1007/978-1-4757-4036-3.

Bowler, S. (2006), "Costs and benefits – Biometrics", available at: https://biometricstoday.weebly.com/costs-and-benefits.html

Brooke, J. (1996), "SUS: a 'quick and dirty'usability", in Usability evaluation in industry, pp. 189-194, available at: www.researchgate.net/publication/319394819_SUS_–_a_quick_and_dirty_usability_scale

Choi, H. and Kwon, H. (2015), "A secure OTP algorithm using a smartphone application".

Chow, Y.W., *et al.* (2015), "A visual one-time password authentication scheme using mobile devices", *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Vol. 8958, pp. 243-257, doi: 10.1007/978-3-319-21966-0_18.

Deborah Golden, C.G. (2015), "Addressing cyber threats Multi-Factor authentication for privileged user accounts contents", available at: www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-federal-cyber-mfa-pov.pdf

Deore, U.D. and Waghmare, V. (2016), "Cyber security automation for controlling distributed data", *2016 International Conference on Information Communication and Embedded Systems, ICICES 2016, (Icices)*, pp. 12-15, doi: 10.1109/ICICES.2016.7518881.

Development, D. (2016), "Multi-factor authentication: a technology whose time has finally come".

Dwivedi, P. and Thomas, G. (2009), "challenges and best practices in kba scheme".

Eldefrawy, M.H., Khan, M.K. and Alghathbar, K. (2010), "One-time password system with infinite nested hash chains", *Communications in Computer and Information Science, 122 CCIS*, pp. 161-170, doi: 10.1007/978-3-642-17610-4_18.

For, A. and Release, P. (2019), "Usability of biometric authentication methods for citizens with disabilities", (June).

Gilsenan, C. (2018), "SMS: the most popular and least secure 2FA method", available at: www.allthingsauth.com/2018/02/27/sms-the-most-popular-and-least-secure-2fa-method/

Gong, L., *et al.* (2013), "A novel one-time password mutual authentication scheme on sharing renewed finite random Sub-passwords", *Journal of Computer and System Sciences*, Vol. 79 No. 1, pp. 122-130, doi: 10.1016/j.jcss.2012.06.002.

Grassi, P.A. *et al.* (2017), "Digital identity guidelines: authentication and lifecycle management", *Special Publication (NIST SP) – 800-63B*, doi: 10.6028/nist.sp.800-63b.

Gunson, N. *et al.* (2011), "User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking", *Computers and Security*, doi: 10.1016/j.cose.2010.12.001.

Hassan, M.A., Shukur, Z. and Hasan, M.K. (2020), "An improved Time-Based one time password authentication framework for electronic payments", *International Journal of Advanced Computer Science and Applications*, Vol. 11 No. 11, pp. 359-366, doi: 10.14569/IJACSA.2020.0111146.

HMAC-based One-Time Password – Wikipedia (2020), available at: https://en.wikipedia.org/wiki/HMAC-based_One-Time_Password

Hsieh, W.B. and Leu, J.S. (2011), "Design of a time and location based One-Time password authentication scheme", *in IWCMC 2011 – 7th International Wireless Communications and Mobile Computing Conference. IEEE*, pp. 201-206, doi: 10.1109/IWCMC.2011.5982418.

Huang, Y., *et al.* (2013), "A new one-time password method", *IERI Procedia*, Vol. 4, pp. 32-37, doi: 10.1016/j.ieri.2013.11.006.

ISO - ISO 9241-11 (2018), available at: www.iso.org/standard/63500.html

Iwasokun, G.B. and Akinyokun, O.C. (2014), "Fingerprint singular point detection based on modified poincare index method", *International Journal of Signal Processing, Image Processing and Pattern Recognition*, Vol. 7 No. 5, pp. 259-272, doi: 10.14257/ijsip.2014.7.5.23.

Jain, A.K., Flynn, P. and Ross, A.A. (2007), "Handbook of biometrics handbook of biometrics", available at: www.springer.com/computer/image+processing/book/978-0-387-71040-2

Jang-Jaccard, J. and Nepal, S. (2014), "A survey of emerging threats in cybersecurity", *Journal of Computer and System Sciences*, Vol. 80 No. 5, pp. 973-993, doi: 10.1016/j.jcss.2014.02.005.

Jeff Sauro (2011), "MeasuringU: Measuring usability with the system usability scale (SUS)", available at: https://measuringu.com/sus/

Joshi, M., Mazumdar, B. and Dey, S. (2018), "Security vulnerabilities against fingerprint biometric system", *arXiv*, pp. 1-27.

Kainda, R., Flechais, I. and Roscoe, A.W. (2010), "Security and usability: analysis and evaluation", *in ARES 2010 - 5th International Conference on Availability, Reliability, and Security*, pp. 275-282, doi: 10.1109/ARES.2010.77.

Kim, H., *et al.* (2020), "Applied sciences analysis of vulnerabilities that can occur when generating One-Time password", doi: 10.3390/app10082961.

Komanduri, S., *et al.* (2019), "Of passwords and people: measuring the effect of password-composition policies", *ACM International Conference Proceeding Series*, Vol. 91 No. 12, pp. 2595-2604, doi: 10.1145/3359789.3359828.

Kumar, R. (2020), "Orientation local binary pattern based fingerprint matching", *SN Computer Science*, Vol. 1 No. 2, doi: 10.1007/s42979-020-0068-y.

Kuo, W.C. and Lee, Y.C. (2007), "Attack and improvement on the one-time password authentication protocol against theft attacks", *Proceedings of the Sixth International Conference on Machine Learning and Cybernetics, ICMLC 2007*, 4, pp. 1918-1922, doi: 10.1109/ICMLC.2007.4370461.

Lal, N.A., Prasad, S. and Farik, M. (2016), "A review of authentication methods", Vol. 5 No. 11, pp. 246-249.

Lashkari, A. and Farmand, S. (2009), "A survey on usability and security features in graphical user authentication algorithms", *Science and Network Security*, Vol. 9 No. 9, pp. 195-204, available at: www.researchgate.net/publication/213217397_A_survey_on_usability_and_security_features_in_graphical_user_authentication_algorithms/file/60b7d51aca56729f63.pdf

Li, Y., *et al.* (2010), "Research on the S/KEY one-time password authentication system and its application in banking and financial systems", *Proceeding - 6th International Conference on Networked Computing and Advanced Information Management, NCM 2010*, pp. 172-175.

Li, Y., Mandal, M. and Lu, C. (2013), "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*, pp. 1439-1443, doi: 10.1109/ICASSP.2013.6637889.

Licenses, D.S. (2020), "The secure technology alliance pushes for digital driver's licenses", *What's Next Media and Analytics, LLC*.

Lone, S.A. and Mir, A.H. (2019), "A stable and secure one-time-password generation mechanism using fingerprint features", *International Journal of Innovative Technology and Exploring Engineering*, Vol. 8 No. 9, pp. 2431-2438, doi: 10.35940/ijitee.i8919.078919.

Magalhães, F., Oliveira, H.P. and Campilho, A.C. (2009), "A new method for the detection of singular points in fingerprint images", *in 2009 Workshop on Applications of Computer Vision, WACV 2009*, p. 5, doi: 10.1109/WACV.2009.5403106.

Mathews, M.M. and Panchami, V. (2017), "Date time keyed – HMAC", *Proceedings of 2016 Online International Conference on Green Engineering and Technologies, IC-GET 2016*, pp. 1-5, doi: doi: 10.1109/GET.2016.7916689.

Mehraj, T., *et al.* (2015), "Contemplation of effective security measures in access management from adoptability perspective", *International Journal of Advanced Computer Science and Applications*, Vol. 6 No. 8, pp. 188-200, doi: 10.14569/ijacsa.2015.060826.

Moon, K.Y., *et al.* (2012), "Biometrics information protection using fuzzy vault scheme", *in 8th International Conference on Signal Image Technology and Internet Based Systems, SITIS 2012r. IEEE*, pp. 124-128, doi: 10.1109/SITIS.2012.28.

N. Haller, B. (1995), "The S/key One-Time password system, tools.ietf.org", available at: https://tools.ietf.org/html/rfc1760

O'Gorman, L. (2005), "Comparing passwords, tokens, and biometrics for user authentication", *Bipin Kumar – Academia.edu*, Vol. 91 No. 12, pp. 2021-2040, available at: www.academia.edu/654335/Comparing_passwords_tokens_and_biometrics_for_user_authentication

Oh, J., Lee, U. and Lee, K. (2019), "Usability evaluation model for biometric system considering privacy concern based on MCDM model".

Ometov, A., *et al.* (2018), "Multi-factor authentication: a survey", *Cryptography*, Vol. 2 No. 1, pp. 1-31, doi: 10.3390/cryptography2010001.

Ometov, A. and Bezzateev, S. (2017), "Multi-factor authentication: a survey and challenges in V2X applications", pp. 129-136.

Oruh, J.N. (2021), "Three-Factor authentication for automated teller machine system", (December 2014).

OS Timeline (2020), "Mobile operating system – Wikipedia", available at: https://en.wikipedia.org/wiki/Mobile_operating_system (accessed 25 October 2020).

Paper, S., Stewin, P. and Seifert, J. (2013), *'SMS-Based One-Time Passwords: Attacks and Defense*, pp. 150-151.

Reese, K.R. (2018), "Evaluating the usability of Two-Factor authentication".

Rydell, J., Pei, M. and Machani, S. (2011), "TOTP: Time-Based One-Time password algorithm", available at: www.scinapse.io/papers/2254700249

S/KEY – Wikipedia (2020), available at: https://en.wikipedia.org/wiki/S/KEY

Sabzevar, A.P. and Stavrou, A. (2008), "Universal Multi-Factor authentication using graphical passwords", pp. 625-632, doi: 10.1109/SITIS.2008.92.

Sanyal, S., Tiwari, A. and Sanyal, S. (2010), "A multifactor secure authentication system for wireless payment", *In Advanced Information and Knowledge Processing*, pp. 341-369, doi: 10.1007/978-1-84996-074-8_13.

Son, J.Y., *et al.* (2019), "A practical challenge-response authentication mechanism for a programmable logic controller control system with one-time password in nuclear power plants", *Nuclear Engineering and Technology*, Vol. 51 No. 7, pp. 1791-1798.doi: 10.1016/j.net.2019.05.012.

Suker, L. (2019), "The security of SMS one time Password – Blog – MEF", available at: https://mobileecosystemforum.com/2019/04/18/the-security-of-sms-one-time-password/

Thomas, N. (2020), "How to use the system usability scale (SUS) to evaluate the usability of your Website – Usability geek", available at: https://usabilitygeek.com/how-to-use-the-system-usability-scale-sus-to-evaluate-the-usability-of-your-website/

Towhidi, F. *et al.* (2011), "The knowledge based authentication attacks", *World Congress in Computer Science*. available at: www.lidi.info.unlp.edu.ar/WorldComp2011-Mirror/SAM8123.pdf

Turn, T. (2020), *Still relying on knowledge-based authentication? Let ' s review the primary problems with KBA: what do you suggest*. available at: https://medium.com/turn-technologies/still-relying-on-knowledge-based-authentication-12dfa376ff26 (accessed 25 March 2021).

Uludag, U. *et al.* (2004), "Biometric cryptosystems: issues and challenges", *in Proceedings of the IEEE*, doi: 10.1109/JPROC.2004.827372.

Uludag, U. and Jain, A.K. (2004), "Attacks on biometric systems: a case study in fingerprints", *Security, Steganography, and Watermarking of Multimedia Contents VI*, Vol. 5306, p. 622, doi: 10.1117/12.530907.

Vic Berger (2007), "Biometrics security technology: the future now", available at: www.securitymagazine.com/articles/78591-biometrics-security-technology-the-future-now-1

Wang, S.J. and Chang, J.F. (1996), "Smart card based secure password authentication scheme", *Computers and Security*, Vol. 15 No. 3, pp. 231-237, doi: 10.1016/0167-4048(96)00005-3.

Xiaoyi Duan, B.N. (2016), "A change pasword attack ressistant scheme for remote user authentication using smart card", *in Proceeding of ICOAC2016*, pp. 269-272.

Yoo, C., Kang, B.T. and Kim, H.K. (2015), "Case study of the vulnerability of OTP implemented in internet banking systems of South Korea", *Multimedia Tools and Applications*, Vol. 74 No. 10, pp. 3289-3303, doi: 10.1007/s11042-014-1888-3.

Zabala-Blanco, D., *et al.* (2020), "Fingerprint classification through standard and weighted extreme learning machines", *Applied Sciences (Sciences)*, Vol. 10 No. 12, doi: 10.3390/APP10124125.

Zulkarnain, S., *et al.* (2013), "A review on authentication methods", *Australian Journal of Basic and Applied Sciences*, Vol. 7 No. 5, pp. 95-107.

Corresponding author
Sajaad Ahmed Lone can be contacted at: sajaadlone@iust.ac.in