Current Multi-factor of Authentication: Approaches, Requirements, Attacks and Challenges

Ali Hameed Yassir Mohammed[1], Rudzidatul Akmam Dziyauddin[2], Liza Abdul Latiff[3]
Razak Faculty of Technology and Informatics-University Technology Malaysia, Kuala Lumpur, Malaysia[1, 2, 3]
College of Computer Science and Information Technology-University of Sumer, ThiQar, Iraq[1, 2]

***Abstract*—Now-a-days, with the rapid and broad emergence of local or remote access to services on the internet. Authentication represents an important security control requirement and the MFA is recommended to mitigate the weaknesses in the SFA. MFA techniques can be classified into two main approaches: based biometric and non-biometric approaches. However, there is a problem to maintain the tradeoff between security and accuracy. The studies that have been reviewed on both authentication mechanisms are found contradictory in the direction of others. In the direction of authentication-based biometrics the researchers tended to increase the recognition accuracy, while in the other direction, the researchers proposed to combine many authentication factors to increase the security layers. The main contribution of this survey is to review and spotlight on the current state of the arts in both authentication mechanisms to achieve a secure user identity. This paper provides a review of authentication protocols and security requirements. In addition to a detailed review with a comparison of secure one-time passcode generation and distribution. Furthermore, a comprehensive review of cancelable biometrics techniques, attacks, and requirements. Finally, providing a summary of key challenges and future research directions.**

***Keywords*—MFA; authentication; OTP; cancelable; biometrics; security; identity**

I. Introduction

Lately, organizations worldwide have made a quantum leap in terms of online application as services expand to the customers' satisfaction [1]. This led to the manifestation of widespread modernized applications as example, users can easily perform various operations such as withdrawal, payment, and transfer over internet banking websites [2]. With the increment of using smartphone devices, authentication protocols can be classified into two approaches non-biometrics-based approach and based biometrics approach [3].

Online identity access management (IAM) is one of the most important services that require customer authentication during daily transactions of funds in a secure way [4]. Some current surveys emphasized various types of customer authentication protocols used for secured data transfer including Single Factor Authentication (SFA) and Multi-Factor Authentication (MFA). For instance, [5] elaborated in detail the significance of various factors used for authentication and compared these factors based on different parameters such as universality, uniqueness, collectability, performance, and usability. The evolution mechanism of the authentication systems is explained in [6] where MFA was implemented for the user and Vehicle-to-Everything (V2X) interactions. A framework was proposed to identify the missing factors and further authenticate the users without supplying any sensitive biometric information. Consequently, it enabled an elastic in-car verification of the occupant using efficient integrated sensors.

In [1] authors analyzed the situation of 30 banks regarding the MFA execution in online banking, wherein the main aim was to determine the impact of the MFA protocols on the regulations, practices, and system security against attacks in the banking sector. It was acknowledged that although it is difficult to implement the MFA systems, wide adoption of the validators taking advantage of the inheritance factors can improve both the security and efficiency of the MFA systems. Broader adoption of authenticators that take the advantage of inheritance factors can improve the security and intricacy of the MFA systems. In the context of mobile devices, a comprehensive survey was conducted on the behavioral patterns of biometrics and constant verification methods [7]. In addition, the behavioral biometrics and verification of the mobile device; various methods of behavioral biometrics and feature extraction were analyzed with a focus on machine learning (ML) models' performance. The limitations of the ML models were discussed with respect to their usage due to the security, and usability as well as privacy concerns.

Also, [8] reviewed the current trends of various MFA protocols and analyzed the gaps in the current literature for future studies related to the perception of users' risks. Different identifiable trends in the MFA studies were found, indicating the need for new validation techniques. However, it lacked risk perception analysis. This work disclosed the presence of cultural and demographic biases in the user study designs. In general, a recruitment bias for the users was achieved in the context of an academic background.

While [9] argued that an increasement in the attacks against the MFA mechanism is mainly related to the nature of the authentication protocols, factors, and their importance for the security of the advent of mobile money. The study conducted a literature review of the attacks and countermeasures in the MFA for mobile money. The authors recommended for a future authentication system use a secure multifactor authentication scheme Personal Identification Number (PIN), One Time Passcode (OTP), and biometrics features. Moreover, protect data during distribution and storage using end-to-end encryption methods. Furthermore, it was stated that despite the coverage of several attacks against mobile money other attacks must be considered. Some of best practices are recommended by [10] to overcome the drawbacks of several mitigation strategies. Meanwhile, the implementation of many countermeasures like new families of hash functions was recommended for security. The study [11] presented a survey of the Cancelable Biometric (CB) methods of various types based on cryptography, filtering, transformation, multi-models, and hybrid methods. It also addressed requirements and performance measures as well as attacks and challenges.

Most of the related surveys are in the field of non-biometric factors and concern the issues related to the improvement of the authentication by improvement of MFA-based OTP generation and distribution. In the second direction, the studies tackle the authentication-based current trend of cancelable biometrics methods. Secure digital identity management is the main aspect of any authentication system that cannot be ignored [12].

Thus, this study refers to the most common performance metrics, requirements, and attacks for both approaches of the related studies [1], [4], [5], [6], [7], [8], [9], [10], and [11].

Although multifactor authentication is a growing and prospective research scope but lacks a comprehensive survey on this field is not available except for fewer research. This survey has made the following contributions:

- The paper has presented a comprehensive survey of both multi-factor of authentication approaches and the state of arts; MFA-based biometrics and non-based biometrics.
- Comprehensive review of various security attacks and performance measures used in CB.
- Comprehensive review of various security attacks and performance measures used in non-based biometrics approaches.

Section II provides a review of identity access management and discusses the authentication protocols, authenticators' classification, Authentication security requirements, and attacks with countermeasures. Section III presents MFA features, Biometrics types, requirements, attacks, and performance metrics of conventional and current trends of cancelable biometrics, and Section IV provides a review of the current state of the arts of cancelable biometrics approaches. Section V describes the authentication of non-based biometrics and provides a security analysis of the current OTP generation and distribution methods. Section VI emphasizes the key challenges. Section VII concludes the paper and presents the future directories.

II. Identity Access Management Protocols

An Identity Access Management Protocol (IAM), is a controlled access that manages the identity provider (Idp), controls the client authentication (signed in), and authorizes (permissions) the use of the targeted resources. IAM organizes the resource's availability, and accessibility and preserves data privacy [4].

IAM protocols permit the digital verification of a client based on several factors. The recent advancement in innovative communication, security authentication, computerized e-payment, and smartphone devices faced increasing authentication challenges due to diverse security threats from attackers or phishers [13].

A conventional SFA approach can keep approved access, login, or get to the secret content by utilizing a single factor-like username and password. Now, this approach was hardened by utilizing at least two factors in the combination process [14]. According to National Institute of Standards and Technology (NIST), the digital identity of a user is defined as a series of functions of authentication, authorization, and accounting of a client in a specific context in a unique way (for example a payment service) [4].

The authentication of the digital identity of a user is achieved in practice via the so-called authentication protocol to get authorization to get access granted to the resources (data, computer program, call object, or procedure). The access server is explained in [1] where requests additional user information for example in the earlier application layer protocol Remote Authentication Dial-In User Service protocol (RADIUS), OpenID, Kerberos, OAuth delegation framework…..etc. Modern identity providers (Idp) rely on Role-Based Access Control (RBAC) to access resources.

Access control utilizes authentication to verify the user identity (uid). In addition, the accounting process is the job to manage and keep the records of the user or any other related objects and works to provide an assertion of the authorized object to the Service Provider (SP) [15].

Furthermore, there are many protocols used to manage the assertion or to transfer the attributes pairs names and values like Security Assertion Markup Language (SAML) protocol. SAML protocol transfers the authentication, attribute, and authorization decision statements from the Idp to SP to perform an action on the requested resource among the relying parties as in Single Sing on (SSO) protocol [16].

SSO is supported by Azure Active Directory (Azure AD) SAML authentication sends requests AuthnRequest (authentication request) and receives the responses from the Idp (Azure AD), Fig. 1 describes the SSO processes sequences to use HyperText Transfer Protocol (HTTP) to post and bind the responding to the SP [16].

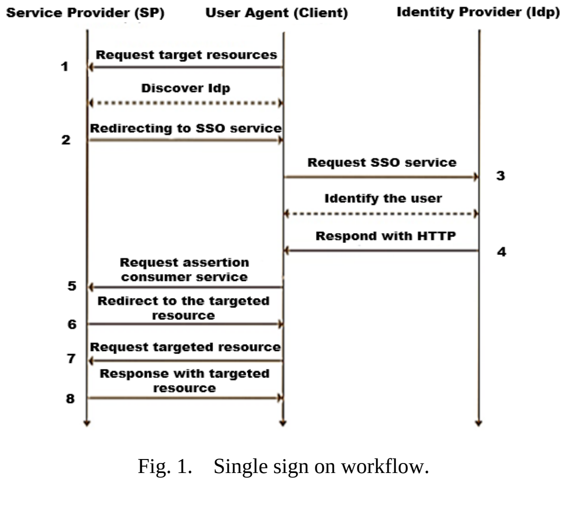

Fig. 1. Single sign on workflow.

A. Authenticators Classification

Authenticators can be classified into different categories such as memorized and look-up secrets, out-of-band devices, token devices, and software as shown in Fig. 2. The salient attributes of these authenticators are briefly described hereunder [1].

1) Memorized secret: When a client shares memorable pieces of information with the server he/she has to recall including passwords, PINs, pass-phrases, and secret questions. The old methods keep the memorized secrets through encryption or salting. However, according to the recommendations of NIST, the memorized secrets must be stored in a form that can withstand both online/offline attacks. In addition, it must be hashed via the approved hash function [17].

2) Look-up secret: It can be electronic records of a secret set shared between the client and server to attest to a possession factor. Then to complete the transaction, the client has to provide the secret associated with definite positions in the records [18]. For example, the user or applicant may be asked by the verifier to give certain subsets of the alphanumerical characters or strings printed on a card in a tabular format [19].

3) Authenticator device: A small hardware device is used to generate an authenticator output. This authenticator platform may be constructed into a specific user's device and employed on the connected devices whereas the roaming verifier links to a device platform via transport protocols [20].

4) Software authenticator: It is sometimes called a software token, wherein the programs are executed to generate the authenticator's output. The software authenticator act as the coordinate of verifier devices for both SFA and MFA software authenticators. The authenticator based on the software may be implemented on laptops, tablet computers, or smartphones. For instance, a mobile application on the user's smartphone can be considered a kind of phone-based authenticator [21]. For security purposes and to prevent unauthorized access to the private or secret data domain, an authenticator based on the software might employ the Trusted Platform Module (TPM) on the client device or trusted execution environments of the processor. Authenticator devices or hardware are classified into SFA and MFA types as explained below [22]:

a) MFA is known as a Time based OTP key (TOTP) token. When the TOTP devices or software share the user's OTP periodically, OTP will be popped up to the user or reach his email or SMS box. Then, the user should manually enter the OTP into the input text box for the successful execution of an MFA protocol completely [22].

b) Using MFA, various devices or software generate tokens in the form of alpha-numeric string which needs some PIN, biometric or secret data for activation, thereby confirming both ownership [22].

5) Out-of-band device: These types of authenticators are shared exclusively over the specific secondary channels (for example an SF device) that approve the possession factor initiated by a secondary mobile phone network channel. Usually, this kind of authenticator depends on a SIM card [4]. The MFA methods rely on mobile phones app where some depend on notification or OTP authentication (event and time-based). Upon receiving the OTP generated by the server and dynamical sharing the user can go for the online transaction [17]. The SMS notification is subjected to security concerns as analyzed afterward. The main flaw in the authentication process is that the user must carry many hard tokens for a different account like Universal 2'nd Factor of authentication (U2F), Near Field Communication (NFC) devices, or Secure Digital (SD) cards. Another threat to the authentication of the user's account is related to the loss or theft of these devices. In addition, many organizations prohibit carrying the electronic devices to or outside the workplace due to security policies. Due to this reason, most of the mobile phones do not have flash memory ports. One cannot upgrade or update the hard tokens because they require a new hard token for each account up-gradation or reconfiguration [2]. High costs are involved in purchasing or exchanging tokens of this type.

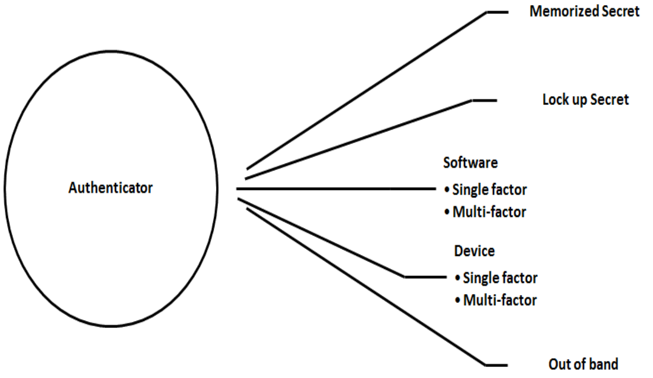

Fig. 2. Authenticator's classification.

The MFA scheme for mobile and smartphones gives an option for the dedicated physical device. For the authentication process, one can use the security tokens in the dedicated device (only known by the individual user) and a one-time password usually 4 to 6 digits [23]. This OTP is sent to the mobile device of the customer via SMS. In short, smartphones are beneficial because the customer carries them most of the time and are free of cost [24], [25]. Regardless of the popularity of SMS verification, it is recognized as the most widely adopted method for user account authentication [2]. Google and Apple introduced an SFA process for their users with the notification of new events when OTP is being delivered to the user's phone. The SMS application depends entirely on the security of the mobile phone operating system [26].

B. Security Requirements and Attacks

The most organization today focuses on information security policies to protect their data as the Confidentiality Integrity Availability (CIA) model or Availability Integrity Confidentiality (AIC) triad Fig. 3. Confidentiality, integrity, and availability objectives should be taken together to provide information security [27]:

1) Confidentiality: The sensitive and personal data of the user should be secured from illegitimate access where the failure to protect the data means there is a data breach or success of the adversary to get access to the data. Impersonating, replay masquerade, spoofing, social engineering, and phishing are the most common attacks against confidentiality. While using Encryption, Quick Response code (QR), Biometrics, username, and password represent the common countermeasures techniques against these types of attacks [3].

2) Integrity: The security control must be able to protect the data from being modified which means the accuracy of the reverted computational outcomes upon saving or transmitting the data over networks. Insider intruders or external Man-in-the-Middle (MITM) are the common types of attacks against integrity. While encryption of the data and error detection in the transmission are common countermeasure techniques against these types of attacks [27].

3) Availability: To ensure the authenticated user accessibility to the resources at need or the reliability of the system uptime. Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) are common attacks against availability. While virtual systems are the common techniques to keep availability [28].

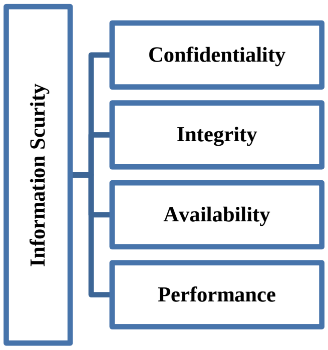

Fig. 3. CIA security requirements model.

Performance: Besides security requirements, it is important to refer to the most common requirement to implement and evaluate any authentication system performance. In addition to recognition patterns performance that its indicators can evaluate the system's ability to distinguish among the users to reduce the EER of biometric systems [29].

III. Multifactor of Authentication Types

Authentication occurs when a user is prompted during the sign-in process to different kinds of resources like networks, devices, or apps that require the client to provide the identity. Using this identity, the client can access these resources together with authenticity proof [30] such as entering a code in the cellphone of the user or scanning a fingerprint. A basic form of authentication requires only one feature or factor, typically a password. To add another security layer, access to various resources might need over and above one factor so-called MFA whenever several factors of evidence are required [22]. There are many types of MFA as described below in Fig. 4.

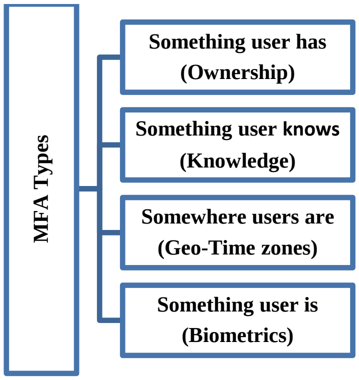

Fig. 4. MFA types.

A. *Something the user has (Ownership)*

Some physical things the user owns like a secret code flash drive, bank Automatic Teller Machines (ATM) card, credit card, master or visa debit cards, or hard tokens. In this regard, the Universal 2'nd Factor (U2F) is an open standard that secures the transaction. It can be designed using USB or similar security technology-based Near Field Communication (NFC) devices [4], and the main drawback where the devices are stolen or lost without enough strength encryption.

B. *Something the user Knows (Knowledge)*

Some knowledge that only the user knows includes the password, PIN, secret question, answer, and so forth wherein the knowledge-based is the most commonly used. Herein, the user needs to reveal secret knowledge for obtaining the authentication. The password strength (complexity) represents the measure of how effectively a password can resist brute force and guessing attacks. Passwords require the use of long and random char types that are not found in the usual dictionary and might enforce the attackers to attempt all probable values [27], [31].

C. *Somewhere users are (Geo-Time-Zone)*

Employment of the user's geographical position acts as a location-based factor that deals with the customer's location at the login session including the physical location of the user. Upon being securely connected to the server, the user is only allowed to log in using the PIN code. While connected to the network the user might have to enter the password if necessary. This can be appropriate as access to the server for monitoring the plan depending on the time zone for the user [32], [33].

D. *Something user is (Biometrics)*

This type represents the biometric features that can be classified into the physical characteristics (biometrics) of the user like the fingerprints, iris, voice, facial, tongue, ears, and the vascular and micro medical biometrics like DNA, and ECG. The second type is the behavioral biometrics like typing speed, keystroke patterns, emotions, signature, gait, voice, height, gender, ethnicity, and so on are in the domain of something the user is. Biometric modal can be classified into two main types Unimodal and Multimodal [34].

1) Unimodal represents a single biometric feature.

2) Multimodal biometric systems Multimodal biometrics are developed by combining many biometrics features.

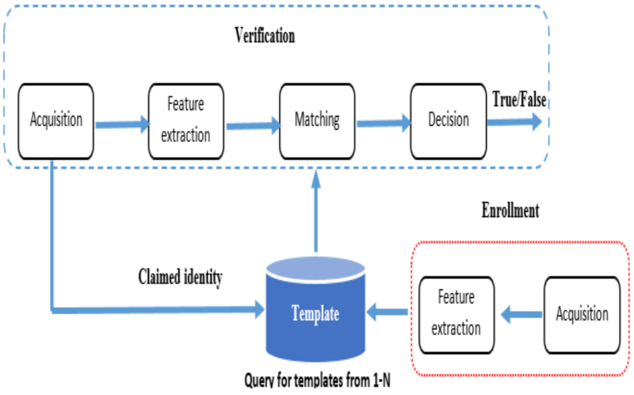

Fig. 5. Biometric system stages.

For authentication, multimodal biometrics features can be combined through fusion at different levels; sensor level, Feature-extraction level, Matching-score level, and Decision level [35]. Biometrics identity verification techniques can be used to measure the features of a user through sequences of processes Fig. 5 [36].

1) Acquisition stage: in a biometric system the first is to acquire the bio-data of users by sensors. For face and iris images, the sensor is typically a camera, the sensor like a camera is typically used to capture the face and iris, and the scanner is used for fingerprints and a microphone for voice. the quality of sensors has a significant impact on the performance of acquisition bio-data as environmental conditions like different sources of noises impacted the brightness, resolution of the captured image, or the depth per inch (dpi) [11] and [37].

2) Feature extraction stage: pre-processed to remove noise and abnormalities from the acquired bio-data to extract the bio-features for the individual ideally and uniquely. Like the fingerprint minutiae point where the position and orientation are used in the fingerprint image system to store these points during user enrollment.

3) Matching and decision stage: In this stage decision of accepting or rejecting is based on the matching scores comparing the features values of the stored template against the score that is generated from the enrolled stages comparing the matching score to a fixed threshold, the scores should be high to indicate the degree of similarity of the same individual (genuine matching) [38].

E. Biometric System Requirements

1) Uniqueness: The use of biometric features to identify the user's digital identity is one of the authentication methods, which must be unique, but twins can have identical features, and therefore the methodology is considered incomplete without adding other biometric factors such as fingerprints [11].

2) Collectability: The process of acquiring biometric properties should be easy, especially when assembled for a database system, and here it needs to be more acceptable.

3) Performance: As we have reviewed, the biometric system must achieve high accuracy and must be with low errors or failure to enroll, which represents the main concern of researchers and the extended challenge, Failure to Enroll (FTE), and an increase in the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are among the challenges that constitute an added burden when designing multifactor authentication systems because the error is costly to the system and lead to invocate algorithms and other supporting methods when accessing the system [35].

4) Spoofing: There can be no guaranteed biometrics system. With the presence of various fraud methods, signatures can be forged, voices can be imitated, and fraud remains one of the most challenging attacks, as these attacks must be addressed [7].

In addition to the usual context of biometric requirements, the new requirements of the cancelable biometric systems.

1) Non-inevitability: original biometric template should be computationally hard to be recovered from the transformed if got compromised [11] and [29].

2) Diversity: should not use the identical biometric template in wide applications to prevent the reusability of the compromised templates [11] and [29].

F. Attacks on Biometrics System

Many attacks on the biometric system could attack at the sensor level like spoofing attacks, another at the application level like brute force attacks, and the database levels like inverse, pre-image, and dictionary attacks. Replay, presentation, MITM, and eavesdropping attacks are other types that thread the network and data transmission which can be countered through utilities time stamp or transmit the encrypted data over a secure channel [39]. On the other hand, clients’ fears of bio-data breaches are one of the new challenges that the International Organization of the Red Cross has indicated, which is the refugees’ fear of leaking their vital data upon receiving financial support from the organization, even in cases related to their biometric data and medical data [40].

The stolen and exposure of biometric data is not a theoretical concern, there are many existing real-world examples, in 2015 about six million fingerprints of people associated with the U.S. government sector of Office of Personnel Management breach. In 2019 of Suprema’s BioStar 2 about 1 million fingerprints, as well as facial recognition information records, are stolen from the publicly accessible database [40]. In 2020 and according to Kaspersky’s analysis, Kaspersky researchers referred that 37% of the servers that process and store biometric data were the target of malware attacks. [41] RSA Conference in San Francisco, In February 2019, the security expert demonstrated the success of real-time attacks like social engineering schemes, phishing SMS and emails, session hijack, and MITM attacks to intercept the traffic to circumvent the MFA[41] and [42]. In academic research, many attacks are proposed as [43] proposed an attack that used the distribution of order statistics to reverse the protected iris template of the ordinal ranking value of the original stored iris templates. The proposed reverse-attack successes to recover greater than 95% of the template and can correctly correlate two templates of 100%. The author in [44] proposed MFA authentication of cancelable biometric hashing mechanism against the attacker is assumed to know the user's password that is bound in the bio-hash code of the face image, the scheme is based on 1-bit compressed sensing signal reconstruction by reducing the number of measurements required to acquire signals through sensing and achieved high security

G. Biometrics System Performance Metrics

NIST SP 800-63B referred that biometrics can be utilized as important factors together with other factors (something users know). Furthermore, according to ISO/IEC 2382-37, in identification matching and authorization, the choice of the threshold value should be assigned carefully in a closed group of 0 for no match and 1 for the full match, an intruder or imposter matching score that exceeds the threshold give high FAR or the False Match Rate (FMR), while the genuine that less than the threshold gives high FRR or the False Non-Match Rate (FNMR) [42]. While the False positive (FP) denotes that exceeding the threshold of imposter scores, the False Negative (FN) sign that genuine client scores are below the threshold. Where the true positive refers to the genuine client and the true negative represents the imposter client [11], [36]. The relation of total scores can be defined in the below functions to measure the performance metrics:

- False Acceptance Rate/ False Positive Rate

$$FAR=FP/FP+FN \quad (1)$$

$$FAR = FPR = FMR * (1 - FTA) \quad (2)$$

- False Reject Rate (FRR)/ False Negative Rate(FNR)

$$FRR/FNR=FN/TP+FN \quad (3)$$

- True Acceptance Rate (TAR) or Genuine Accept Rate (GAR)

$$TAR = 1 - FRR \quad (4)$$

$$FRR=FNR= FTA + FNMR * (1 - FTA) \quad (5)$$

- True Acceptance Rate (TAR) or Genuine Accept Rate (GAR)

$$TAR = 1 - FRR \quad (6)$$

- Half Total Error Rate (HTER)

$$HTER=FNMR + FMR/2 \quad (7)$$

- Failure to Enroll rate (FTE): represents the total number of the user's failed attempts to enroll in the bio-system successfully or the number of unsuccessful attempts to enroll in the bio-system.

- The Receiver Operating Characteristic (ROC): this curve can plot the FMR on X-axis while plotting the FNMR along the Y-axis, or FAR vs FRR, or TAR vs the FAR.

- Equal Error Rate: It is another performance measurement to evaluate recognition where the FAR and FRR are equal.

$$\text{Accuracy}=\text{TP}+\text{TN}/\ TP + FP + TN + FN \quad (8)$$

- Training Time: is the time of the learning algorithm to training data.

- Testing Time: this is the time of the process to test data in the learning algorithm.

IV. Authentication-based Cancellable Biometrics Approaches

The current trend of authentication research is to integrate biometric data through cancelable mechanisms that should fulfill the aforementioned cancelable biometrics requirements in subsection E of Section III. The concept of cancelability is derived from the concept of one-way functions through Cartesian, polar, functional, and hybrid transformations, but the disparity in the entries of the same user (intra-user variations) and subject to errors, and that is what we have been observed in most of the researches that attempts to improve the methods of transformation through two main approaches BioHashing, and BioEncodding [11]. [37] proposed cancelable biometrics based on a Hill cipher transformation of the biometric signals of face and palmprint as multimodal. The author in [45] proposed to use the deep Convolution Neural Network (CNN) to protect the face templates based on random projection. The first extract is the features vector from the face image with 224*224 VGG face input. then, during the training of 15 layers 4096-dimensional output with dimensions of 1599*4096 is projected randomly then reducing the dimension of the feature vector to 1024, the deep CNN is trained (to predict the binary code) by set neuron values to 1 if the threshold is 0.5 and 0 for else. Then the proposed deep CNN can remove the redundancies feature vector. [46] proposed cancelable biometric-based feature random projection to protect the template data against the Attack via Record Multiplicity (ARM), when the adversary may succeed to obtain multiple transformed templates from different applications to retrieve the original feature vector, which is critical to privacy and identity requirements. The basic matrix is connection with local feature slot to generate the key that is discarded after the use.

A valuable privacy-preserving research [47] proposed an authentication biometric key agreement based on cancelable biometrics. The proposed scheme integrated fuzzy commitment and Elliptic Curve Cryptography (ECC) cipher to guarantee the security of users' bio-templates against cybercrime thefts. the scheme is utilized the Random Distance Method (RDM)to generate non-invertible templates by using a random grayscale salting matrix that is added to the original feature vector values, then performing the median filter to divide each vector into two equal-size vectors to get the pseudo-biometric template.

In addition, [48] proposed protecting the transformed iris template by using ordinal ranking after XORed the user-specific string with the IrisCode string. Another proposal by [49] is to get better performance by enhancing Index First One

(IFO) hashing for iris templates. The binary confidence matrix considered the variation in noisy iris Biometric Template Protection (BTP) systems. the Fully Connected Architecture (FCA) and Bilinear Architecture (BLA) are used by [50] to hash a binary vector template. The proposed framework based on Deep Neural Networks (DNN) was tested on 50 subjects only. The author in [51] proposed a Multi-Instance Cancelable iris authentication Deep Learning (MICBTDL) and used a CNN (triplet loss) and trained to differentiate a positive image from a negative on IITD and MMU iris dataset images. Both [52] and [53] proposed to encrypt the Iris Codes using classical cryptography algorithms.

Table I presents the summarization regarding CB systems and provides an overall idea about the recent direction of authentication-based CB. Ten recent works have been summarized based on four categories which are: “purpose of the research”, then “proposed methods”, “Bio-Feature”, “Bio-Dataset” and finally “**Performance**” measurement of the research that has been used in the experiment.

TABLE I. SUMMARY ANALYSIS OF THE RECENT CB SCHEMES

Ref.	**CB Scheme**	**Bio-Features**	**Bio-Dataset**	**Performance**

[37]	Hill Cipher	Face
		Palmprint
			Face={ORL, Indian Face, Yale}
			Palmprint={PolyU, CASIA}
				EER

[49]	Confidence matrix	Iris	CASIA Iris v4-interval	EER
[45]	Random projection	Face	CMU-PIE, FEI, Color-FERET	GAR
[46]	Feature-adaptive random projection	Fingerprint	FVC2002 DB1-DB3 and FVC2004 DB2	EER
[52]	Encryption (3DES+Twofish)	Iris	CASIA-IrisV3	GAR

[47]	Random distance method (RDM)	Fingerprint
		Face
		Iris
			Fingerprint={FVC2006}
			Face={CASIA-Face V5}
			IRIS={IRIS(LWIR)}
				FAR, EER, ROC communication computational

[53]	Encryption (AES)	Iris	CASIA-IrisV3	EER
[48]	Local rank	Iris	CASIA Iris v3-interval	EER

[50]	Deep neural networks Integration	Face
		Iris
			Face={ Casia-Webface}
			Iris={CASIA-Iris-Thousand}
				GAR

[51]	MICBTDL	Iris	IITD+ MMU	EER

V. NON-BIOMETRICS AUTHENTICATION METHODS

Previous literature demonstrates authentication-based cancelable biometrics to account for authentication mechanisms and the current methods to enhance the pattern recognition of biometric features.

In this section, non-based biometrics authentication methods have been summarized according to the methods for generation and distribution. Also, tabular evaluation matrices have been summarized in each section. These evaluation matrices provide a structured technique for the outcome of the metrics and the criteria of the proposed methods. In OTP Authentication Procedure The server customer or application (Object/Service) as a client has to register an online account and provide the mobile number and other required information during the registration process so that online login to the bank server (as an example) is successful (Fig. 6).

1) The server exchanges the OTP code with the registered mobile number, email, or application, and the code is used as a second layer of the authentication mechanism for any transaction achieved through the following steps [10], [54].

2) The client requests a transaction to connect with the server using his credentials username and password.

3) The server checks the client validity and if successful then initiates the OTP generation algorithm.

4) The output of step ii should be encrypted using cryptography algorithms (Symmetric or Asymmetric) or hashing then forward to the client.

5) The client's application decrypts the obtained OTP if it is encrypted on the server side.

6) The client's application gets the OTP code in step 4 and enters it manually or automatically in the text box of the bank application.

7) The server receives the code from the client then checks the comparison condition if success then completes the transaction during the timer period. The server should acknowledge the client for the verification of the transaction status (success or failure).

Steps 2 and 3 being optional are recommended according to NIST special publication 800-63B privacy requirements [55] against various attacks such as birthday, offline/online guessing, impersonation, rainbow, a man in the middle, key-recovery, and collision types.

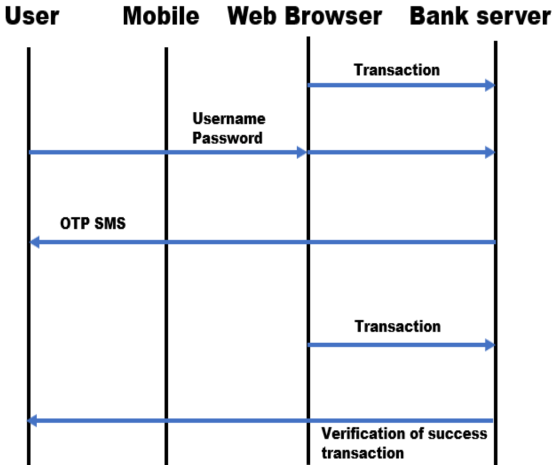

Fig. 6. One-time passcode workflow.

B. *One-Time Passcode Generation Methods*

The first attempt to overcome the weaknesses of finite OTP generation for authentication was by [56] using a hush chain. The author in [57] proposed a model to generate OTP. The model addresses the weaknesses of the Lamport method when finite generation OTP and used the hash chain function. However, the bottleneck of the proposed model is the server generates an unlimited OTP code for each client login. The author in [58] proposed a model to overcome the weaknesses of the OTP model of Lamport using a Merkle tree an L-divided tree (with the binary tree), and the hash chain. The author illustrated the proposed model examples without implementation. A model was proposed [59] for generating the OTP using the following steps. The first step was based on the certification authority's client login details user name and password and converting it to 8 bits. The second step converted the message's length to 8 bits. In the third step, a binary code is converted to decimal base (CB2D) was used to convert 16 bits (2 × 8 bits) to base decimal, the conversion result is two 3 decimal digits. Fourth step used 3 Vedic multipliers to get the OTP multiplied by two decimal digits. The proposed OTP generation method used the user name and the password credentials without encryption.

A novel method was introduced [60] for improving the verification in mobile banking using lightweight and solid OTP generators. The OTP generation model is based on three client factors (6 digits of the last transaction date DD: MM: YY. The last transaction amounted to 16 digits, wherein three login characters of the password were selected. The client must have an SD card containing initialization vectors (IV) set of 256 bits, AES-256-XTS encrypted random keys, each key of 256 bits was divided into two portions, each one containing 128 bits on the user’s side and the other half on the server side. Then it was XOR'ed followed by concatenating and hashing together via the SHA 256 for using the AES-256-CBC to encrypt the OTP. Afterward, it was sent to the client via the internet to the mobile device of the client to make a comparison of the transaction is succeeded. All the used 256 keys were stored in the hardware component SD Card with the bank client. Later, the OTP was sent only through the internet only when the client application initiates a session of user online login. OTP length is 64 digits only, without considering using case-sensitive characters like uppercase letters or symbols, charset sizes are medium (0-9, a-z).

An OTP generation scheme is proposed by [31] for authentication purposes. The first step encrypts a randomly selected image stored in the server database using Bitwise Masking Alternate Sequence (BWMAS). A two-step authentication model was proposed to generate the OTP on many intermediate operations. Then in the second stage, OTP was sent by e-mail to the client. The researchers in [61] proposed an algorithm for the implementation of secure OTP generation. OTP was a mixture of the present time value of 3 digits from the login time (HH: MM: SS) to shuffle the hex and octal which is obtained via the back-end server-generated value random operation. This value is 32-bits in size, producing an 8-digit of number combination. Fixed length OTP of 8 digits only is obtained without including the small or capital letters as well as symbols, generating a complexity of 232= 4294967296 combinations.

Table II elucidates the OTP generation using various schemes [59] [60], [31], and [61] including the proposed methods, initial data of OTP generation, encryption mechanisms, hash functions, delivery methods types such as email, SMS, Internet, and the authentication protocol.

C. One-Time Passcode Distribution Methods

First, the client has to enroll in the first phase at the server for receiving the OTPs. In addition, the client must declare the procedure of distributing the OTP via his/her email or SMS, or some apps [57]. An approach was proposed [62] for online e-banking authentication using OTP. This approach provided a mechanism for the generation of an infinite and forward OTP utilizing SHA3 and SHA2 followed by the dynamical concatenation understandable by humans. An inimitable verification scheme was employed with a distinct initial seed for generating several OTPs on the users’ mobile devices. This method showed superior performance compared to the existing authorization techniques. This is due to the eradication, during the authorization process, of cellular networks. The findings that are critical for online transactions have shown a high degree of success and efficacy in the verification and authorization.

TABLE II. SUMMARY ANALYSIS OF DIFFERENT EXISTING ONE-TIME PASSCODE GENERATION STUDIES

Ref.	Methods	Initial data	Cryptography	Hash Functions	Media	Authentic ation
[59]	CBCD and 3 *3 Vedic Multiplier	Client's User name and Password	No	No	Internet	MFA
[60]	The OTP generation model is based on client factors and then encrypted and hashed them and forwarded to the server-side as a 64digits length	selected three client factors: last transaction date DD: MM: YY, Last transaction amount to 6 bits, three login password characters	AES-256	SHA2-256	SMS	MFA
[31]	OTP is generated by applying Bit-wise Masking and Alternate Sequence (BWMAS) on selecting a random image stored at the server database Provided by Clients to generate numeric OTP.	Biometric Fingerprint	No	No	Email/SMS	MFA
[61]	Server-generated random value OTP would be a combination of the current time value of 3 digits from the login time to shuffle the hex and octal to that combined value. This value is 32-bit in size, which produces an 8-digit number combination	Current Time of login session HH:MM: SS	No	No	SMS	MFA

The OTP is sent via cellular data to the client, without using encryption methods to protect data privacy. Generally, the methods for the OTPs distribution are multiple and have their own merits. The business organization looks for a method of OTP verification distribution, especially via SMS and email. The OTP-based SMS is usually utilized for the users' login and password resetting. Several organizations particularly the financial sectors send the OTPs via SMS and email as an additional confirmation step for the users. The following modes are used:

1) Email-Based: The OTP can be delivered to the client through his/her Email [63].

2) SMS Based: The OTP can be delivered to the client through his mobile phone over-the-air SMS or delivered to an OTP application [63].

3) Push notifications: These can be sent to the client's registered smartphone for out-of-band authentication which could not be intercepted at the point of password entry when the client approves the request. Then, the authentication application informs the server that the client is confirmed. The authentication-based push notification provides a higher level of security since it addresses the most important SMS and email shortcomings, such as vulnerability to replay attacks. It is even faster than typing in a passcode [64], [65].

4) Hard copies: Some banks provide clients with hard-printed OTPs for each transaction [63].

Many methods are used to distribute an SMS or email wherein each has its weaknesses. The OTP distribution schemes are simpler for the companies because of the abundance of the SMTP to SMS channels. No setting is required for the clients wherein they just request a code to log in. The ease of administration related to the delivery of OTPs via SMS and email is frequently utilized, enabling temporary access. Nonetheless, OTP is MFA which is something that the user knows, and the mobile devices (phones, computers, smart-watches, tablets, and so forth) something that the user is not essentially true.

Using email and SMS delivery protocols (something one has) the OTP is sent to the user. Presently, several phone numbers can be cloned which affects the authentication of the client identity [66], [67]. In this regard, email phishing, spear-phishing, and scammers can develop ways that entice the clients to enter a username or password and follow a suspicious link or download malware applications. Thus, visiting certain authentic-looking websites permits the adversary to steal the credentials or gain control of the users' devices [62], [63].

The OTP overcomes the shortcomings of the SFA like traditional password because it's not reusable and it can be distributed through the Out of Bound (OOB) channel as well as not vulnerable to replay attacks. Therefore, it's more secure to transmit an OTP over a push notification. Due to the rapid adoption and fast growth of push authentication, it offers a low-cost, easy-to-use, and secure substitution for email and SMS distribution methods [68].

Table III shows the comparison of main property qualities such as security, message size, feedback possibilities, response time, and cost among SMS, email, and push notifications. It is argued that push notification is the best method that could be used for OTP distribution due to the low cost, high speed, and more secure than other methods of OTP distribution. While in [69] the authors proposed a model to improve the OTP distribution security using Elliptic Curve Cryptography (ECC) and Iris for key generation. The model encrypted the generated OTP and sends it as ciphertext, not as plain text. The use of ECC with the iris code-based public key could encrypt the OTP successfully and send it through email. The author in [70] utilized lightweight cryptography and text steganography to encrypt and hide OTP to send the stego text as an SMS to the mobile application of the client. This method was used to protect the delivery of OTP SMS where the OTP was encrypted and steganography ciphering was exploited for hiding it in a standard SMS. This process used the Date of Birth (DOB) of the customer with the secret four digits of PIN only as a key to encrypt and decrypt the OTP. The author in [71] proposed a mechanism for protecting OTP delivery from many types of attacks, especially smartphone Trojans. A virtual dedicated channel was used to secure SMS-based OTPs against cell phone Trojans stealing SMS. By assigning a port to transmit and receive OTP via TCP/ UDP from the service provider, and protect the mobile application's storage files internally.

Table IV enlists the secure end-to-end distribution of OTP [69], [70], [71] based on many categories such as proposed methods, encryption mechanisms, hash functions, delivery methods types (for example email, SMS, internet), and authentication protocol.

TABLE III. COMPARISON OF MAIN QUALITIES IN ONE-TIME PASSCODE DISTRIBUTION STUDIES

Parameter	SMS	Email	Push Notification
Security [20]	Medium	Low	High
Message size [72]	Limited (140 Bytes)	Long	Moderate (according to app settings).
Feedback Possibilities [73], [74]	Yes (If the sender is Known)	Yes (If the sender is Known)	Yes (according to app settings).
Response Time [73], [74]	Medium	Low	High
Usability of intuitive user interfaces[75]	Medium	Low	High
Cost [76]	High	Low	Low

TABLE IV. SUMMARY ANALYSIS OF DIFFERENT ONE-TIME PASSCODE DISTRIBUTION STUDIES

Ref.	**Methods**	**Initial data**	**Cryptography**	**Hash Functions**	**Media**	**Authentication**
[60]	Traditional OTP Generation and Distribution	Numeric (0-9)	No	No	SMS	MFA
[69]	Secure OTP distribution	Iris of client	Elliptic Curve Cryptography (ECC)	No	Email	MFA
[70]	Secure OTP distribution	Client date of Birth DOB	Steganography fixed key, lightweight Feistel cipher	No	Internet	MFA
[71]	OTP distribution	Assign a port to receive OTP in the user client's mobile phone	No	No	Use a virtual dedicated channel from ISP	MFA

VI. MAIN CHALLENGES

The combination of new solutions is always challenging for both developers and managers for the implementation of a strong identity in usability and resistance against known attacks [5]. So it is worth mentioning that issues for authentication must be tackled regarding the other digital identity management mechanisms in authentication.

A. This Paper has Concerned the MFA Regarding the Cancelable Biometrics Approach and Shows the following Challenges

1) Most of the biometric databases vary in type and version while low accuracy when in real use, beside train biometric recognition systems through machine learning or deep learning results in varying accuracy metrics.

2) Choosing a set of biometric features to design appropriate authentication systems is a critical challenge in designing MFA based on multimodal cancelable biometrics.

3) Low user adaptability due to additional hardware requirements for sensing and processing persists despite smartphone applications.

4) Concerns increase for biometric data leakage despite cancelable biometric requirements.

5) Difficulties in pattern recognition due to the noise, or the variations of large intraclass of transformed templates.

B. In the Second MFA Approach (Non-based Biometrics)

The main challenge of non-based biometrics is explained in [77] where the impossibility of distinguishing the correlation between the ideal-random and pseudo-random sequences in the absence of unlimited computational capacity. While in some cases the clients may be unable to access the OTP codes offline or without a network (for example in an airplane during international journeys) [78].

In addition to the growth and success of session hijacking attacks, research on both approaches did not concern this type of attack. The surveyed studies did not concern with its proposing of authorization and accounting mechanisms, most of them were simulated without paying attention to the impacts of decision-making (only pattern recognition enhancement) by the identity provider based on the backend database and customer account data as well as the target resource, because the accessing to a particular resource must direct the matcher according to the conditions of access controls policies to direct or redirect the accessing of one or several resources.

Circle of verification and loop of authentication, this means without a controller or police (based biometric or non-based biometric) in algorithm design, the enrollment and verification of the client identity will repeat and will call or invocate the system resources (objects, algorithms, procedures) that require access from one moment to another and between one object and another, and this is costly due to consume the two parties of the communication system resources. While the researchers in [79] pointed threat of involving third-party authentication, especially when this requires the customer's biometric data. Also, the research [79] indicated one of the main challenges today is to ensure that the customer's biometric data is destroyed and not used again (no copy of such biometric data on the server side), and to confirm that to the customer.

VII. CONCLUSION AND FUTURE DIRECTORIES

The digital identities and MFA are intensively combined in the context of advanced information communication technologies. This paper comprehensively reviewed various MFA in two approaches biometric and non-biometric mechanisms besides pointing out many standard protocols. Effective non-biometrics MFA schemes are required to combine many factors and protocols to secure the data distribution in an end-to-end. Cancelable biometrics approaches are proposed to transform the templates like iris to be difficult to obtain the original traits but still suffer from difficulties to maintain the tradeoff between security and performance while supporting effective biometrics recognition as shown in the literature. Also, we presented different performance measures used for cancelable biometrics in both identification and verification. Now, we also draw attention to future directions in cancelable biometrics. The readers may look for propose new mechanisms to transform the templates and maintain the recognition performance while protecting the privacy of biometric data. The employment of deep learning in CB requires a large number of training samples. In some cases there is only a single trait for each subject is available that imposes limits and constraints on the training. However, the future of MFA appears boundless with absolutely secured data exchange over the internet and cellular. Concisely, the ongoing extensive research activities in the MFA are likely to transform many facets of the forthcoming evolution and continue to be more secure.

REFERENCES

[1] F. Sinigaglia, R. Carbone, G. Costa, and N. Zannone, “A survey on multi-factor authentication for online banking in the wild,” Comput. Secur., vol. 95, 2020, doi: 10.1016/j.cose.2020.101745.

[2] F. Liébana-Cabanillas, I. R. de Luna, and F. Montoro-Ríosa, “Intention to use new mobile payment systems: A comparative analysis of SMS and NFC payments,” Econ. Res. Istraz. , vol. 30, no. 1, pp. 892–910, 2017, doi: 10.1080/1331677X.2017.1305784.

[3] T. Mehraj, M. A. Sheheryar, S. A. Lone, and A. H. Mir, “A critical insight into the identity authentication systems on smartphones,” Indones. J. Electr. Eng. Comput. Sci., vol. 13, no. 3, pp. 982–989, 2019, doi: 10.11591/ijeecs.v13.i3.pp982-989.

[4] P. A. Grassi, M. E. Garcia, and J. L. Fenton, “Digital identity guidelines: revision 3,” Digit. Identity Guidel., vol. 58, no. 2, pp. 130–137, 2020, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

[5] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, “Multi-Factor Authentication: A Survey,” Cryptography, vol. 2, no. 1, p. 1, 2018, doi: 10.3390/cryptography2010001.

[6] A. Ometov and S. Bezzateev, “Multi-factor authentication: A survey and challenges in V2X applications,” Int. Congr. Ultra Mod. Telecommun. Control Syst. Work., vol. 2017-Novem, pp. 129–136, 2017, doi: 10.1109/ICUMT.2017.8255200.

[7] I. Stylios, S. Kokolakis, O. Thanou, and S. Chatzis, “Behavioral biometrics & continuous user authentication on mobile devices: A survey,” Inf. Fusion, vol. 66, no. February 2020, pp. 76–99, 2021, doi: 10.1016/j.inffus.2020.08.021.

[8] S. Das, B. Wang, Z. Tingle, and L. Jean Camp, “Evaluating user perception of multi-factor authentication a systematic review,” arXiv, 2019.

[9] G. Ali, M. A. Dida, and A. E. Sam, “Two-factor authentication scheme for mobile money: A review of threat models and countermeasures,” Futur. Internet, vol. 12, no. 10, pp. 1–27, 2020, doi: 10.3390/fi12100160.

[10] H. Shahriar, T. Klintic, and V. Clincy, “Mobile Phishing Attacks and Mitigation Techniques,” J. Inf. Secur., vol. 06, no. 03, pp. 206–212, 2015, doi: 10.4236/jis.2015.63021.

[11] Manisha and N. Kumar, “Cancelable Biometrics: a comprehensive survey,” Artif. Intell. Rev., vol. 53, no. 5, pp. 3403–3446, 2020, doi: 10.1007/s10462-019-09767-8.

[12] R. Y. Zakari, A. Suleiman, Z. K. Lawal, and N. Abdulrazak, “A Review of SMS Security Using Hybrid Cryptography and Use in Mobile Money System,” Am. J. Comput. Sci. Eng., vol. 2, no. 6, pp. 53–62, 2015.

[13] M. Noman Riaz and A. Ikram, “Development of a Secure SMS Application using Advanced Encryption Standard (AES) on Android Platform,” Int. J. Math. Sci. Comput., vol. 4, no. 2, pp. 34–48, 2018, doi: 10.5815/ijmsc.2018.02.04.

[14] A. Saha and S. Sanyal, “Survey of Strong Authentication Approaches for Mobile Proximity and Remote Wallet Applications - Challenges and Evolution,” Int. J. Comput. Appl., vol. 108, no. 8, pp. 10–15, 2014, doi: 10.5120/18930-0319.

[15] I. Amazon Web Services, “AWS Identity and Access Management: Benutzerhandbuch,” p. 2106, 2020.

[16] P. Pandey and T. N. Nisha, “Challenges in Single Sign-On,” J. Phys. Conf. Ser., vol. 1964, no. 4, 2021, doi: 10.1088/1742-6596/1964/4/042016.

[17] E. B. Barker, M. Smid, and D. Branstad, “NIST Special Publication 800-152 - A Profile for U. S. Federal Cryptographic Key Management Systems,” NIST Spec. Publ., 2015, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-152.pdf.

[18] E. Barker, A. Roginsky, G. Locke, and P. Gallagher, “Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths,” NIST Spec. Publ., vol. 1, no. January, pp. 800–131, 2011.

[19] E. Belmekki, B. Raouyane, A. Belmekki, and M. Bellafkih, “Secure SIP signalling service in IMS network,” 2014 9th Int. Conf. Intell. Syst. Theor. Appl. SITA 2014, no. May, 2014, doi: 10.1109/SITA.2014.6847291.

[20] P. Doucek, L. Pavlíček, J. Sedláček, and L. Nedomová, “Adaptation of password strength estimators to a non-english environment—the Czech experience,” Comput. Secur., vol. 95, 2020, doi: 10.1016/j.cose.2020.101757.

[21] A. S and K. S. Anil Kumar, “Security and performance enhancement of fingerprint biometric template using symmetric hashing,” Comput. Secur., vol. 90, 2020, doi: 10.1016/j.cose.2020.101714.

[22] Shally and G. S. Aujla, “A review of one time password mobile verification,” Int. J. Comput. Sci. Eng. Inf. Technol. Res., vol. 4, no. 3, pp. 113–118, 2014.

[23] S. Ma et al., “An empirical study of SMS one-time password authentication in android apps,” ACM Int. Conf. Proceeding Ser., pp. 339–354, 2019, doi: 10.1145/3359789.3359828.

[24] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, “Security analysis of mobile two-factor authentication schemes,” Intel Technol. J., vol. 18, no. 4, pp. 138–161, 2014, [Online]. Available: http://ezproxy.library.capella.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=iih&AN=97377858&site=ehost-live&scope=site.

[25] N. R. Dive, M. D. Likhar, N. A. Ughade, S. S. Chune, and M. Khonde, “Survey Of Graphical Password Authentication Techniques,” no. 3, pp. 145–152, 2016.

[26] H. S. Alsaiari, “Graphical One-Time Password Authentication,” 2016.

[27] M. Botacin, F. Ceschin, P. de Geus, and A. Grégio, “We need to talk about antiviruses: challenges & pitfalls of av evaluations,” Comput. Secur., vol. 95, 2020, doi: 10.1016/j.cose.2020.101859.

[28] B. A. Buhari, A. A. Obiniyi, K. Sunday, and S. Shehu, “Performance Evaluation of Symmetric Data Encryption Algorithms: AES and Blowfish,” Saudi J. Eng. Technol., vol. 04, no. 10, pp. 407–414, 2019, doi: 10.36348/sjeat.2019.v04i10.002.

[29] S. Mansfield-Devine, “The ever-changing face of phishing,” Comput. Fraud Secur., vol. 2018, no. 11, pp. 17–19, 2018, doi: 10.1016/S1361-3723(18)30111-8.

[30] Y. Shah, V. Choyi, A. U. Schmidt, and L. Subramanian, “Multi-factor authentication as a service,” Proc. - 2015 3rd IEEE Int. Conf. Mob. Cloud Comput. Serv. Eng. MobileCloud 2015, no. March, pp. 144–150, 2015, doi: 10.1109/MobileCloud.2015.35.

[31] J. Bhaumik and I. Chakrabarti, Communication , Devices , and Computing. 2017.

[32] M. Conti, N. Dragoni, and V. Lesyk, “A Survey of Man in the Middle Attacks,” IEEE Commun. Surv. Tutorials, vol. 18, no. 3, pp. 2027–2051, 2016, doi: 10.1109/COMST.2016.2548426.

[33] E. De Cristofaro, H. Du, J. Freudiger, and G. Norcie, “A Comparative Usability Study of Two-Factor Authentication,” no. March, 2014, doi: 10.14722/usec.2014.23025.

[34] A. Lumini and L. Nanni, “Overview of the combination of biometric matchers,” Inf. Fusion, vol. 33, pp. 71–85, 2017, doi: 10.1016/j.inffus.2016.05.003.

[35] V. Conti, C. Militello, F. Sorbello, and S. Vitabile, “A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems,” IEEE Trans. Syst. Man Cybern. Part C Appl. Rev., vol. 40, no. 4, pp. 384–395, 2010, doi: 10.1109/TSMCC.2010.2045374.

[36] R. Dwivedi and S. Dey, “A non-invertible cancelable fingerprint template generation based on ridge feature transformation,” vol. 4, pp. 1–17, 2018, [Online]. Available: http://arxiv.org/abs/1805.10853.

[37] H. Kaur and P. Khanna, “Non-invertible biometric encryption to generate cancelable biometric templates,” Lect. Notes Eng. Comput. Sci., vol. 1, no. 1, pp. 432–435, 2017.

[38] M. A. Al-Shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, “An efficient identity-based conditional privacy-preserving authentication scheme for secure communication in a vehicular ad hoc network,” Symmetry (Basel)., vol. 12, no. 10, pp. 1–25, 2020, doi: 10.3390/sym12101687.

[39] A. O. Alaswad, A. H. Montaser, and F. E. Mohamad, “Vulnerabilities of Biometric Authentication ‘Threats and Countermeasures,’” Int. J. Inf. Comput. Technol., vol. 4, no. 10, pp. 947–958, 2014, [Online]. Available: http://www.irphouse.com.

[40] B. Hayes(ICRC), “Facilitating innovation, ensuring protection: the ICRC Biometrics Policy - Humanitarian Law & Policy Blog | Humanitarian Law & Policy Blog,” 2019. https://blogs.icrc.org/law-and-

policy/2019/10/18/innovation-protection-icrc-biometrics-policy/ (accessed Aug. 23, 2021).

[41] "Five ways to hack MFA and the FBI's mitigation strategy."

[42] T. Seals, "ThreatList: A Third of Biometric Systems Targeted by Malware in Q3 | Threatpost," 2019. https://threatpost.com/threatlist-a-third-of-biometric-systems-targeted-by-malware-in-q3/150778/ (accessed Aug. 23, 2021).

[43] O. Ouda, "On the Practicality of Local Ranking-Based Cancelable Iris Recognition," IEEE Access, vol. 9, pp. 86392–86403, 2021, doi: 10.1109/access.2021.3089078.

[44] B. Topcu, C. Karabat, M. Azadmanesh, and H. Erdogan, "Practical security and privacy attacks against biometric hashing using sparse recovery," EURASIP J. Adv. Signal Process., pp. 1–20, 2016, doi: 10.1186/s13634-016-0396-1.

[45] A. K. Jindal, S. Rao Chalamala, and S. K. Jami, "Securing Face Templates using Deep Convolutional Neural Network and Random Projection," 2019 IEEE Int. Conf. Consum. Electron. ICCE 2019, 2019, doi: 10.1109/ICCE.2019.8662094.

[46] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A cancelable biometric authentication system based on feature-adaptive random projection," J. Inf. Secur. Appl., vol. 58, p. 102704, 2021, doi: 10.1016/j.jisa.2020.102704.

[47] L. Wu, L. Meng, S. Zhao, X. Wei, H. Wang, and L. Wu, "Privacy-preserving Cancelable Biometric Authentication Based on RDM and ECC," IEEE Access, 2021, doi: 10.1109/ACCESS.2021.3092018.

[48] D. Zhao, S. Fang, J. Xiang, J. Tian, and S. Xiong, "Iris Template Protection Based on Local Ranking," Secur. Commun. Networks, vol. 2018, 2018, doi: 10.1155/2018/4519548.

[49] T. Y. Chai, B. M. Goi, and W. S. Yap, "Towards better performance for protected iris biometric system with confidence matrix," Symmetry (Basel)., vol. 13, no. 5, 2021, doi: 10.3390/sym13050910.

[50] V. Talreja, M. C. Valenti, and N. M. Nasrabadi, "Multibiometric secure system based on deep learning," 2017 IEEE Glob. Conf. Signal Inf. Process. Glob. 2017 - Proc., vol. 2018-Janua, pp. 298–302, 2018, doi: 10.1109/GlobalSIP.2017.8308652.

[51] M. Sandhya, M. K. Morampudi, I. Pruthweraaj, and P. S. Garepally, "Multi-instance cancelable iris authentication system using triplet loss for deep learning models," Vis. Comput., 2022, doi: 10.1007/s00371-022-02429-x.

[52] O. C. Abikoye, U. A. Ojo, J. B. Awotunde, and R. O. Ogundokun, "A safe and secured iris template using steganography and cryptography," 2020.

[53] A. A. Asaker, Z. F. Elsharkawy, S. Nassar, N. Ayad, O. Zahran, and F. E. Abd El-Samie, "A novel cancellable Iris template generation based on salting approach," Multimed. Tools Appl., vol. 80, no. 3, pp. 3703–3727, 2021, doi: 10.1007/s11042-020-08663-6.

[54] I. Standard, "INTERNATIONAL STANDARD ISO / IEC Information technology — JPEG 2000," vol. 2007, 2007.

[55] J. L. Fenton et al., "Digital identity guidelines: Authentication and Lifecycle Management," NIST Spec. Publ. 800-63B, pp. 2–79, 2017, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[56] L. Lamport, "Password Authentication with Insecure Communication," Commun. ACM, vol. 24, no. 11, pp. 770–772, 1981, doi: 10.1145/358790.358797.

[57] C. S. Park, "One-time password based on hash chain without shared secret and re-registration," Comput. Secur., vol. 75, pp. 138–146, 2018, doi: 10.1016/j.cose.2018.02.010.

[58] Y. Suga, "An Extended Lamport-Like One-Time Password Scheme and its Applications," 2018 IEEE Int. Conf. Consum. Electron. - Asia, ICCE-Asia 2018, pp. 6–9, 2018, doi: 10.1109/ICCE-ASIA.2018.8552134.

[59] S. P. Shyry, M. Mahithaasree, and M. Saranya, "Implementation of One Time Password by 3∗3 Vedic Multiplier," 2nd Int. Conf. Comput. Commun. Signal Process. Spec. Focus Technol. Innov. Smart Environ. ICCCSP 2018, no. Icccsp, 2018, doi: 10.1109/ICCCSP.2018.8452861.

[60] H. S. Elganzoury, A. A. Abdelhafez, and A. A. Hegazy, "2018 , 35 th NATIONAL RADIO SCIENCE CONFERENCE A New Secure One-Time Password Algorithm for Mobile Applications 2018 , 35 th NATIONAL RADIO SCIENCE CONFERENCE," no. Nrsc, pp. 249–257, 2018.

[61] "Gosavi, S. S., & Shyam, G. K. (2020). A Novel Approach of OTP Generation Using Time-Based OTP and Randomization Techniques. In Data Science and Security (pp. 159-167). Springer, Singapore.," 2020.

[62] S. Hussain, B. U. I. Khan, F. Anwar, and R. F. Olanrewaju, "Secure Annihilation of Out-of-Band Authorization for Online Transactions," Indian J. Sci. Technol., vol. 11, no. 5, pp. 1–9, 2018, doi: 10.17485/ijst/2018/v11i5/121107.

[63] M. M. Hashim, M. Shafry, and M. Rahim, "a Review and Open Issues of Diverse Text," vol. 96, no. 17, pp. 5819–5840, 2018.

[64] M. Sahin, A. Francillon, P. Gupta, and M. Ahamad, "SoK: Fraud in Telephony Networks," Proc. - 2nd IEEE Eur. Symp. Secur. Privacy, EuroS P 2017, pp. 235–240, 2017, doi: 10.1109/EuroSP.2017.40.

[65] S. M. Seth and R. Mishra, "Comparative Analysis Of Encryption Algorithms For Data Communication," Ijcst, vol. 2, no. 2, pp. 292–294, 2011.

[66] B. Reaves, N. Scaife, D. Tian, L. Blue, P. Traynor, and K. R. B. Butler, "Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways," Proc. - 2016 IEEE Symp. Secur. Privacy, SP 2016, pp. 339–356, 2016, doi: 10.1109/SP.2016.28.

[67] A. R. L. Reyes, E. D. Festijo, and R. P. Medina, "Enhanced multi-factor out-of-band authentication en route to securing SMS-based OTP," Int. J. Eng. Technol. Innov., vol. 9, no. 2, pp. 145–154, 2019.

[68] P. A. Grassi et al., "NIST Special Publication 800-63B," 2019, Accessed: Jan. 23, 2021. [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[69] "Mahto, D., & Yadav, D. K. (2016). Security improvement of one-time password using crypto-biometric model. In Proceedings of 3rd International Conference on Advanced Computing, Networking and Informatics (pp. 347-353). Springer, New Delhi.," 2016.

[70] S. Chandra and S. Tai, Advances in Intelligent Systems and Computing 828 Proceedings of the 2nd International Conference on Data Engineering and Communication Technology, vol. 2. 2017.

[71] S. Paper, P. Stewin, and J. Seifert, "SMS-Based One-Time Passwords : Attacks and Defense," pp. 150–159, 2013.

[72] A. Hernández-Reyes, G. Molina-Recio, R. Molina-Luque, M. Romero-Saldaña, F. Cámara-Martos, and R. Moreno-Rojas, "Effectiveness of PUSH notifications from a mobile app for improving the body composition of overweight or obese women: A protocol of a three-Armed randomized controlled trial," BMC Med. Inform. Decis. Mak., vol. 20, no. 1, pp. 1–10, 2020, doi: 10.1186/s12911-020-1058-7.

[73] L. G. Morrison et al., "The effect of timing and frequency of push notifications on usage of a smartphone-based stress management intervention: An exploratory trial," PLoS One, vol. 12, no. 1, pp. 1–15, 2017, doi: 10.1371/journal.pone.0169162.

[74] A. Wohllebe, "Consumer Acceptance of App Push Notifications: Systematic Review on the Influence of Frequency," Int. J. Interact. Mob. Technol., vol. 14, no. 13, p. 36, 2020, doi: 10.3991/ijim.v14i13.14563.

[75] V. Picchio, V. Cammisotto, F. Pagano, R. Carnevale, and I. Chimenti, "We are IntechOpen , the world ' s leading publisher of Open Access books Built by scientists , for scientists TOP 1 %," Intechopen, no. Cell Interaction-Regulation of Immune Responses, Disease Development and Management Strategies, pp. 1–15, 2020, [Online]. Available: https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics.

[76] S. M. Abdulhamid et al., "A Review on Mobile SMS Spam Filtering Techniques," IEEE Access, vol. 5, pp. 15650–15666, 2017, doi: 10.1109/ACCESS.2017.2666785.

[77] H. Kim, J. Han, C. Park, and O. Yi, "Analysis of vulnerabilities that can occur when generating one-time password," Appl. Sci., vol. 10, no. 8, 2020, doi: 10.3390/APP10082961.

[78] T. S. Mohamed, "Security of Multifactor Authentication Model to Improve Authentication Systems," Inf. Knowl. Manag., vol. 4, no. 6, pp. 81–87, 2014.

[79] S. Barra, K. K. R. Choo, M. Nappi, A. Castiglione, F. Narducci, and R. Ranjan, “Biometrics-as-a-service: Cloud-based technology, systems, and applications,” IEEE Cloud Comput., vol. 5, no. 4, pp. 33–37, 2018, doi: 10.1109/MCC.2018.043221012.