IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 25 November 2023, accepted 16 December 2023, date of publication 22 December 2023,
date of current version 4 January 2024.

Digital Object Identifier 10.1109/ACCESS.2023.3346045

TOPICAL REVIEW

Online Banking User Authentication Methods: A Systematic Literature Review

NADER ABDEL KARIM[1], **OSAMA AHMED KHASHAN**[2], **HASAN KANAKER**[3], **WALEED K. ABDULRAHEEM**[4], **MOHAMMAD ALSHINWAN**[5,6], **AND ABEDAL-KAREEM AL-BANNA**[7]

[1]Department of Intelligent Systems, Faculty of Artificial Intelligence, Al-Balqa Applied University, Al-Salt 19117, Jordan
[2]Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates
[3]Department of Cyber Security, Isra University, Amman 11622, Jordan
[4]Information Systems and Networks Department, The World Islamic Sciences and Education University, Amman 11947, Jordan
[5]Faculty of Information Technology, Applied Science Private University, Amman 11931, Jordan
[6]MEU Research Unit, Middle East University, Amman 11831, Jordan
[7]AI and Data Science Department, University of Petra, Amman 11196, Jordan

Corresponding authors: Nader Abdel Karim (Nader.salameh@bau.edu.jo) and Osama Ahmed Khashan (okhashan@ra.ac.ae)

ABSTRACT Online banking has become increasingly popular in recent years, making it a target for cyberattacks. Banks have implemented various user authentication methods to protect their customers' online accounts. This paper reviews the state-of-the-art user authentication methods used in online banking and potential cyber threats. This paper starts by exploring different user authentication methods, such as knowledge-based authentication (KBA), biometrics-based authentication (BBA), possession-based authentication (PBA), and other methods. The advantages and disadvantages of each user authentication method are then discussed. Furthermore, the paper discusses the various cyber threats that can compromise user authentication for online banking systems, such as malware attacks, social engineering, phishing attacks, man-in-the-middle (MiTM) attacks, denial of service (DoS) attacks, session hijacking, weak passwords, keyloggers, SQL injection, and replay attacks. Also, the paper explores the user authentication methods used by popular banks, which can provide insights into best practices for safeguarding online banking accounts and future user authentication methods in online banking and cyber threats. It states that the increasing use of BBA, two-factor authentication (2FA), and multi-factor authentication (MFA) will help improve the security of online banking systems. However, the paper also warns that new cyber challenges will emerge, and banks need to be vigilant in protecting their customers' online banking accounts.

INDEX TERMS User authentication, online banking, cyber threats, 2FA, MFA, cyber challenges.

I. INTRODUCTION

The tendency towards online business has grown dramatically in recent years. In the banking sector, where most banks have started to offer their services online, online services are increasingly predominant. According to the Pew Research Center, in reported USA in 2013, 61% of internet users in the USA were using online banking, which is set to rise to 77.6% by 2022 [1]. Online banking, also known as e-banking or Internet banking, is an electronic payment system that enables bank or other financial organization clients to transact over the Internet [2], [3]. Using online banking services, customers can execute online payments and other financial operations, as well as remote access to their bank accounts and additional financial information. Online banking services have susceptible data and online banking tools must be enhanced with effective and reliable security mechanisms. A robust authentication is necessary to provide high security and privacy [4], [5]. The method by which people prove their identity to gain access to online banking platforms is known as user authentication. User authentication methods are used to verify the identity of a user trying to access an online system. There are three main types of user authentication methods: KBA, BBA, and PBA. Recently, 2FA and MFA have become increasingly common [6], [7] (see Figure 1).

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

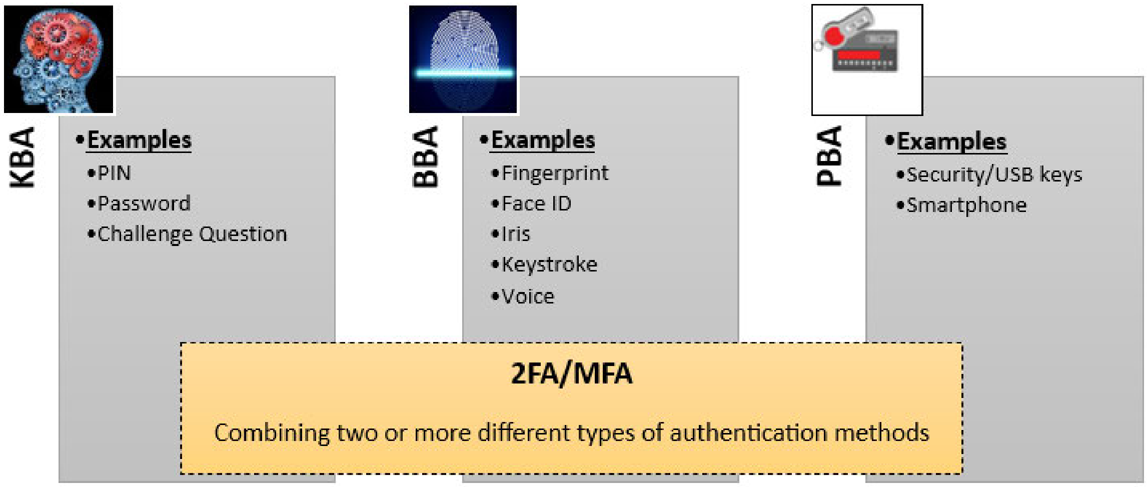

FIGURE 1. **The general user authentication classifications.**

KBA -Something you know- is the most popular user authentication technique because it depends on the user knowing something. It asks the user to enter information that should only be known by them, such as a password, PIN, or challenge question (also known as a security question). KBA is simple to set up and use, but it can be vulnerable to attacks such as guessing, phishing, brute force, and social engineering attacks [7], [8]. BBA -Something you are- is a form of a user authentication technique that relies on what the user is and checks the user's physiological or behavioral characteristics to confirm their identity [9], [10]. The physical characteristics of a user, like fingerprints, facial features, or iris scans, are used in physiological biometrics to confirm their identification. Patterns in the user's voice, keystrokes, and other characteristics can be found using behavioral biometrics [11]. Although BBA can be more intrusive and challenging to implement than KBA, it is more secure [12] PBA, also called a Token -Something you have-, depends on something the user already possesses. The user must own a tangible item, such as a smartphone or a security token. While PBA can be more inconvenient for the user than KBA, it is more secure [4], [8]. This study intends to provide a systematic literature review (SLR) of the various user authentication methods used in online banking systems and investigate potential cyber threats that may threaten and attempt to bypass these methods. Historically, the most common authentication method has been username and password combinations [12]. Nevertheless, the rise of sophisticated cyber threats has shown that relying solely on passwords is insufficient to prevent unauthorized access to user accounts [13], [14]. Two-factor authentication, or 2FA, is an extra layer of security that can be added to your online banking account. It is a security process requiring two pieces of information to verify a user's identity. The first factor is typically a password, while the second factor can be something like a code sent to your phone(One Time Password -OTP), a fingerprint scan, or facial recognition [15], [16]. 2FA is more secure than single-factor authentication (SFA), requiring only one user authentication method, such as a password. This is because even if someone knows your password, they will still need access to your phone or other devices to enter the second factor [8], [17].

Recently, many financial institutions have added a layer of security called MFA to their security systems to contain sophisticated attacks and to add a higher degree of protection to sensitive operations [18], [19]. MFA combines various forms of user authentication (More than two), such as something the user is (biometric data), something the user has (a smartphone or token), and something they know (a password) [13], [20]. An in-depth examination of the various MFA techniques used in online banking will be done in this review, along with an assessment of how well they contribute to user convenience while enhancing security [13], [21].

Moreover, this review will look at newly developed authentication technologies, such as biometrics (fingerprint, facial recognition) and behavioral biometrics (Voice pattern, keystroke dynamics), which are gaining popularity in the online banking industry. These methods use distinctive physiological or behavioral traits to verify a user's identity, providing a more streamlined and secure user experience. Additionally, this review aims to contribute to the present debate on improving online banking systems' security and user experience by exploring emerging technologies and demonstrating threats facing online banking user authentication. Ultimately, the study's findings will aid financial institutions and policymakers in making defensible choices regarding adopting robust user authentication techniques in online banking, ensuring the security of users' financial information in a world that is becoming more interconnected.

The rest of this paper is structured as follows: Section II presents the advance of this paper over existing work, Section III provides the methodology, Section IV demonstrates the analysis and discussion, Section V presents challenges facing online banking user authentication, and Section VI offers the conclusion.

II. ADVANCEMENT OVER EXISTING WORKS

Online banking user authentication is a critical and challenging problem that requires continuous research and development to ensure the security and comfort of online banking customers. However, there is a lack of a complete and up-to-date review of the available literature on this topic. Most earlier review studies need to be updated or focused on a certain type of user authentication technique or model. For example, the authors of [22] and [23] did research on authentication and communications security in online banking. Their publications, however, were published in 2016 and 2018, respectively, and did not incorporate recent advancements and trends in this area. Likewise, authors in [24], [25], and [13] analyzed user authentication models or approaches for online banking, but their papers were limited to a specific component or category of user authentication, such as mobile IMEI number, advanced security solutions, or MFA. Furthermore, other review articles, such as [26], addressed user authentication in general rather than the specific context and limits of online banking. As a result, we accomplished an SLR on online banking user authentication methods from 2013 to 2023. Our SLR is comprehensive and complete, as it covers all types of online banking user authentication methods and categories, including PBA, KBA, BBA, 2FA, and MFA. Our SLR is also innovative and timely in that it gives a review and analysis of the current state-of-the-art online banking user authentication systems, as well as identifying emerging trends, and challenges in this field. We hope that our SLR can contribute to the advancement of knowledge and practice of online banking user authentication methods, as well as clarify and guide future research and development in this field.

III. METHODOLOGY

To survey existing state-of-the-art associated online banking authentication methods, an SLR was accomplished utilizing the procedures mentioned by the EBSE Technical Report [27].

A. RESEARCH QUESTIONS

The main goal of this research is to investigate the current user authentication methods that could be used in online banking systems. This research also focuses on online banking user authentication cyber threats and provides examples of already used user authentication methods by famous worldwide banks. To cover the aims and objectives of this SLR, we pose the following research questions:

- RQ1: What existing authentication methods/techniques can authenticate online banking users?
- RQ2: What potential user authentication cyber threats affect online banking?
- RQ3: What are current user authentication methods used by well-known banks worldwide?

TABLE 1. Search keywords.

No.	String
1	[Online banking, e-banking, internet banking] user authentication methods
2	Authentication of [Online banking, e-banking, internet banking]
3	[Authentication, Verification] of [Online banking, e-banking, internet banking]
4	[Online banking, e-banking, internet banking] threats
5	[Global, well-known] banks, online user authentication methods

B. SEARCH STRATEGY

In this phase, we focused on scientific digital libraries and databases, search keywords, reference management tools, and a search process. We describe each process in the following subsections.

1) SCIENTIFIC DIGITAL LIBRARIES

This review was done on several popular scientific digital libraries and databases in English. The scientific digital libraries and databases searched were Science Direct, Springer Link, IEEE Xplore, ACM, and Google Scholar.

2) SEARCH KEYWORDS

The search keywords were derived from the SLR research questions. We have also included synonyms and alternatives. The synonym keywords are taken from the literature on online banking security topics. Table 1 displays the search keywords used in the above-mentioned digital libraries.

3) REFERENCE MANAGEMENT

In this SLR, the Mendeley Reference Manager v2.90.0 [28] was used as a reference management tool to collect and manage the retrieved scientific papers. It enabled researchers to easily manage, edit, add, and remove documents from the tool's internal database.

4) SEARCH PROCESS

The publishing date range was defined as Jan 2013 through the end of May 2023. The focus was established on articles identified with online banking authentication or threats. All other insignificant articles were omitted. The search was started in Jun 2023. Table 2 demonstrates all results related to each Digital library. The selection of the study involved multiple phases. First, potentially relevant articles were identified using search strings, and then the publication's titles and abstracts were screened. As a result, many papers were omitted; based on their insignificance to the research questions. Next, if there were any suspicions about the potential publication's inclusion, the entire article would be obtained for further evaluation [27].

Complete content scanning was performed on the last set of journals. Thus, a group of publications was involved in the

TABLE 2. Search keywords.

Database Name	No. of articles	Exclude Based on Title	Exclude Based on Abstract	Included articles
IEEExplore	33	22	1	10
Springer Link	164	136	15	13
ScienceDirect	93	70	14	9
ACM	188	154	19	15
Google Scholar	235	187	21	27
Total Articles	**713**	**569**	**70**	**74**

review, depending on its relevance to the research questions and clearance of their objectives and methodology. The total number of papers used in this review (after removing search redundant and missing information papers) was 65 articles.

IV. ANALYSIS AND DISCUSSION

This section presents several samples of data extracted from relevant studies as well as an analysis and discussion of the SLR results. Table 3 summarizes some of the collected literature within three sections: year, reference, and description.

A. USER AUTHENTICATION METHODS IN ONLINE BANKING

This subsection answers RQ1: "*What existing authentication methods/techniques can authenticate online banking users?*" Figure 2 shows the classification of available authentication methods that can be used in online banking, along with user authentication methods proposed by authors of each category.

Figure 2 shows that various online banking user authentication methods are used and categorized into KBA, BBA, PBA, and Other Methods. This classification allows for a comprehensive understanding of the strengths and weaknesses associated with each authentication type, shedding light on the diverse range of methods employed within the online banking sector.

1) KBA METHODS

Under the category of KBA, methods such as passwords, PINs, and challenge questions are commonly used in conjunction with other authentication factors. The PIN is an abbreviation for a personal identification number, a secret number only the customer knows and can use to prove their identity [44]. The security of PIN as user authentication in online banking depends on the length and complexity of the PIN; according to the PCI-DSS standards, which are the global security standards for payment card transactions, PINs should be at least four digits long and should not be based on easily guessed information depends on the length and complexity of the PIN [50]. A password is secret data, typically a string of characters. Generally, passwords provide a higher level of security than PINs due to their length [8], [51]. Passwords are also more complex and challenging to guess because they can contain various characters, including alphanumeric and special characters. However, passwords and PINs can be subject to security breaches if not picked correctly. To maintain maximum security, it's critical to choose a robust password policy (e.g., NIST, OWASP password policy) and choose unique passwords or PINs and update them frequently; also, using passphrases is an excellent option to ensure longer passwords, which makes passwords more difficult to crack [52]. Moreover, Graphical passwords are a way to authenticate users by using images or shapes. They are more secure than passwords and PINs because they are harder to guess or brute-force. This is because there are many more possible combinations of images than there are possible combinations of characters. However, graphical passwords can be harder to remember than passwords and PINs, so it is essential to choose a system that is easy to use and remember [8], [53]. Security questions are an additional layer of security that can help protect your account. However, if the answers to your security questions are easy to guess or find (e.g., in the user's social accounts), they may not be very effective [8]. That's why choosing challenging and unique security questions only you know the answers to is essential. This will help to keep your account safe from unauthorized access.

2) BBA METHODS

In BBA category, both physiological biometrics (such as fingerprint and face ID) and behavioral biometrics (including voice patterns, keystroke dynamics, and tapping behavior) are employed [11], [39], [54], [55]. Physiological biometrics leverage unique biological traits to verify user identity, providing high security. Similarly, behavioral biometrics analyzes user behavior for authentication purposes, offering a robust authentication mechanism, but it raises concerns about privacy and the security of the stored data. Implementing robust measures to protect against unauthorized access or misuse of biometric information [47]. Moreover, implementing biometric authentication can be complex and may not work for all users. Factors such as hardware requirements, accuracy, and user acceptance must be considered when implementing biometrics in online banking systems [56], [57], [58].

3) PBA METHODS

PBA techniques use a physical object or a code that the user owns to confirm their identity. PBA techniques have several benefits and issues [8]. QR code authentication involves scanning a unique QR code to authenticate the user. This can complicate unauthorized access attempts, as the QR code is challenging to replicate. However, there is a risk of QR code copying or theft, which can undermine its effectiveness [59]. One-time password (OTP) authentication generates temporary and exclusive authentication tokens delivered through SMS or email. This method provides an additional layer of security, as the generated OTPs are only valid for a limited time. However, it relies on protecting the communication channels the OTPs deliver [35], [60]. Security/USB keys are physical devices that users possess

TABLE 3. Sample of data extraction.

Year	Ref.	Description
2014	[30]	The authors proposed a secure authentication system that combines a password and a camera-equipped mobile phone as an authentication token using a QR code.
	[31]	The authors proposed a new protocol for user authentication in online banking and electronic payment systems using a specific device called OffPAD. This protocol uses biometrics to generate OTPs that are both secure and privacy-preserving.
2015	[32]	The authors proposed a system that uses the user ID, password, fingerprint, and random strings to protect online banking services.
2016	[33]	The authors illustrated the proposed Challenge Question (CQ) from the dynamic Know Your Customer (KYC) database for transaction authorization to ensure secure and flawless finances.
2017	[34]	The authors use the user ID, password, OTP, mobile number, and geolocation to authenticate the online banking users.
	[35]	The authors use personal devices that utilize different cryptographic primitives, such as encryption, digital signature, and hashing, to authenticate users.
	[36]	The authors proposed a technique for transforming the OTP using lightweight cryptography and hiding the cipher text through text steganography. The transformed OTP is sent as an SMS to the user's mobile device. The ciphering process uses the user's PIN provided by the bank during registration, ensuring end-to-end encryption of the OTP SMS.
2018	[37]	The authors proposed an MFA system for online banking that provides mutual authentication using color recognition, icon recognition, user ID verification, and the secured socket layer.
2019	[38]	The authors presented an authentication scheme that uses MFA authentications based on password, OTP, and fingerprint.
	[39]	The authors presented a behavioural biometric-based user authentication technique for smart device application-level security. Instead of locking the entire device, the technique focuses on safeguarding particular applications. It provides static 2FA (keystroke and mouse dynamics) at the start of an interactive session as well as continuous keystroke authentication throughout the session.
2020	[40]	The authors proposed a 2FA framework using OTP and fingerprints for online payment. The proposed framework uses a secret key exchange between the client and the server and uses a specific password through the algorithm.
	[41]	The authors proposed an MFA authentication scheme using username/password, familiar random images, and fingerprint data. It introduces the Match on Card technique for biometric data protection. Familiar random images enhance security.
2021	[42]	This paper proposed using FIDO, which includes two sub-specifications: 1- Universal Authentication Framework using FIDO registration locally, such as using a fingerprint or PIN with no password. 2- Universal 2nd Factor, FIDO registration using a second-factor device such as a USB key.
	[43]	The authors proposed an MFA method using username/password, user biometrics (fingerprint or facial recognition), and device identification (IP address, cookies, or digital certificate).
	[44]	The authors in this study suggest the usage of mobile screen swipe and touch data for user authentication.
	[45]	The authors in this study proposed using the device's MAC address and mobile International Mobile Equipment (IMEI) as a user authentication method in online banking.
	[46]	The authors proposed a two-level integrated authentication mechanism (2L-IAM). At the first level, the user logs in to their Internet banking portal using a PIN or fingerprint. At the second level, the user is authenticated using face recognition should they initiate a transaction classified as sensitive.
2022	[47]	The authors proposed a keystroke dynamics-based user authentication model as an additional security method to passwords to increase smart devices' security level when using online banking.
	[48]	The authors proposed a 2FA method using images with blockchain and OTP. Authors use image chains for image storage and blockchain for personal information storage (mobile number) to secure the database. The database is stored on an Ethereum-based blockchain. After determining whether the image is fake or real, match the webcam image with the image chain; if both images match, the OTP is given to the user's phone number for login access.
	[49]	The authors proposed a 2FA method for online banking transactions using OTP and fingerprint.
	[50]	The authors proposed an MFA method for online banking using PIN, OTP, and CAPTCHA.
2023	[51]	The authors investigated the feasibility of using voice recognition when spelling out the user PIN as a user authentication method, the results show that the spoken PIN method seems to represent a compromise between security and ease of use. The sophisticated sound authentication was appreciated for its ease of use, but it was also rated worst regarding the perceived security.

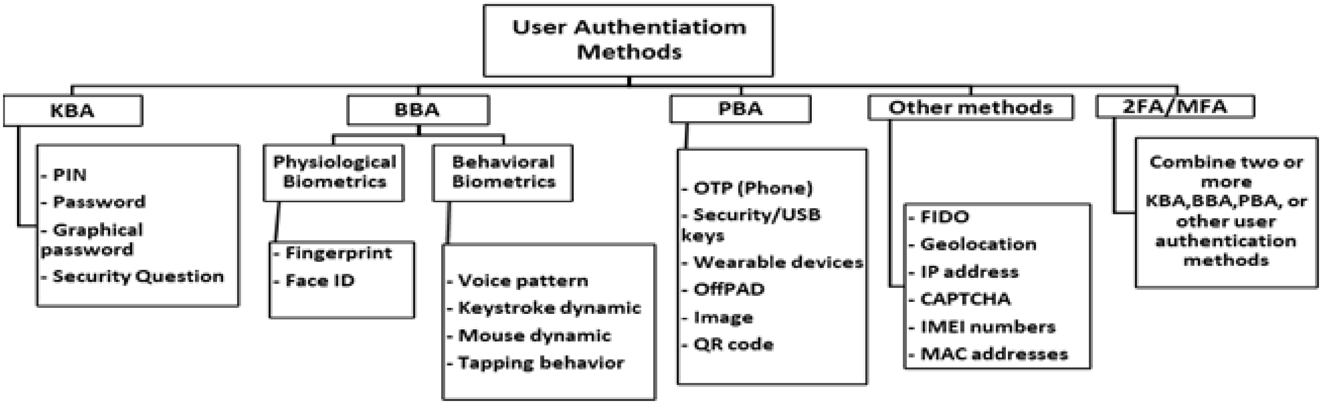

FIGURE 2. Taxonomy of user authentication methods for online banking.

and use for authentication. These keys provide a higher level of security, as they require the physical presence of the key to authenticate. However, the implementation and compatibility of security/USB keys may pose challenges, and users need to ensure the safekeeping of the physical key [40], [61]. Wearable devices, such as smartwatches or fitness trackers, can be used for authentication. These devices leverage the physical presence of the user as an authentication factor. Wearable devices offer convenience and portability but must be securely paired with the user's online banking account to ensure reliable authentication [34], [62]. OffPAD (Offline Personal Authentication Device) is a dedicated device that allows users to authenticate offline. It stores user credentials securely and verifies them without requiring an internet connection. OffPADs provide an additional layer of security by keeping the authentication process isolated from online threats. However, the availability and adoption of OffPADs may vary, and users need access to such devices to benefit from this authentication method [30], [63]. Image-based authentication requires users to possess specific images for authentication purposes. These images serve as a visual representation of the user's identity [46], [64]. While image-based authentication can be convenient for users, it relies on the security of the image database and the potential vulnerability of images being copied or stolen.

4) OTHER AUTHENTICATION METHOD

The "Other Authentication Methods" category includes various techniques, each with its strengths and weaknesses. MAC addresses and IMEI numbers are unique identifiers assigned to devices, which can enhance security measures [65]. However, they are not foolproof, as determined attackers can spoof or change them [43]. IP addresses and geolocation can provide additional security by verifying the user's location [33], [66]. However, they can be masked or manipulated using proxy servers or virtual private networks (VPNs), reducing their effectiveness as standalone authentication methods [41], [67], [68]. CAPTCHA tests, widely used to distinguish between humans and automated bots, typically involve visual or auditory challenges requiring human interpretation [69]. While CAPTCHAs serve as an effective deterrent against bots, advanced algorithms, or Optical Character Recognition (OCR) technology can potentially bypass them, compromising their reliability. FIDO (Fast Identity Online) is another authentication method that uses public-key cryptography and biometrics to provide passwordless authentication [35], [70]. FIDO offers enhanced security by eliminating the need for passwords and relying on solid authentication through biometrics and cryptographic keys. However, FIDO's implementation, infrastructure, and compatibility may pose challenges that must be considered in online banking systems [71].

5) 2FA AND MFA

The system developers commonly integrated the above authentication methods into 2FA or MFA framework [9], [19], [72]. For example, in the KBA category, PINs, passwords, graphical passwords, and security questions were frequently used with other factors. For example, users might be required to enter their PIN and answer a security question to log in to their online banking account. BBA methods, such as fingerprints, facial recognition, and behavioral biometrics, were commonly integrated into MFA or 2FA setups. PBA methods, including OTPs, security/USB keys, wearable devices, and image-based authentication, were often used alongside other factors. Additional techniques like FIDO, QR codes, geolocation, IP addresses, and CAPTCHA were also incorporated into MFA or 2FA setups to enhance security. By combining different types of authentication methods, banks can significantly improve the security of their systems and create a layered security approach that is difficult for attackers to crack. This is because if the attacker compromises one layer, the rest of the layers will protect the system [4], [6], [73]. For example, a user might be required to enter their password and then provide a fingerprint scan to log into a system. This would make it much more difficult for an attacker to access the system, even if they guessed the user's password. So, when online banking adopts the 2FA and MFA, this will establish a comprehensive and robust authentication process, mitigating risks associated with relying solely on a single factor [74], [75], [76].

Table 4 summarizes the strengths and weaknesses of all previously mentioned online banking user authentication methods.

Based on a compilation of 28 research, Table 5 and Figure 3 offer an overview of the authentication methods utilized in online banking user authentication systems. The data obtained from the table offers an in-depth investigation of the authentication techniques used in these systems, complete with matching references. The table illustrates the wide variety of authentication methods that are used to guarantee safe access to online banking services.

The talk that follows looks at the frequency with which specific authentication techniques are applied and how they are integrated in the MFA and 2FA, as shown in Table 5 and Figure 3.

With 12 appearances each, fingerprint and password authentication stand out among these methods as the most frequently used within the MFA and 2FA frameworks. OTPs (SMS) were used nine times and PINs were used six times. Other methods that were commonly used include keystroke dynamics (3 times), offPAD (2 times), IP addresses (2 times), and face ID (2 times). Several authentication methods, including graphical passwords, wearable devices, OTPs (email), challenge questions, voice patterns, mouse dynamics, FIDO, security key/USB devices, tapping behavior, QR codes, MAC addresses, IMEI numbers, geolocation, and CAPTCHA, were mentioned once or used in limited instances.

The repeated usage of passwords, OTP (SMS), and fingerprint as part of MFA highlights their effectiveness in enhancing security. Additionally, the combination of various authentication methods within the MFA and 2FA frameworks exemplifies the significance of implementing layered security measures to protect user accounts and sensitive data in online banking systems. For example, the combination of password and OTP (SMS) was used four times in the table, showing that organizations use layered security measures to protect their systems.

B. THREAT-FACING ONLINE BANKING

In this subsection, we provide answers found regarding RQ2: "*What potential user authentication cyber threats affect online banking?*". Based on the literature [4], [54], [72], [85], [18], [87], [88], [89], [90], [91], [92], [93], [94], [95], [96], [97], [98], [99], [100], [101], [102] the following are the most serious threats that could face online banking:

online banking:

1) MALWARE ATTACKS

Malware poses a significant threat to online banking systems. Attackers can use malicious software to gain unauthorized access to systems. Malware can be utilized to hijack sessions, steal passwords, and even set keyloggers on victims' machines [91], [94], [95], [103], [104].

2) SESSION HIJACKING

The act of gaining unauthorized access to a user's session so that an attacker can exploit the user's identity and access their online bank account is referred to as "session hijacking." Via network connection interception or the use of vulnerabilities, attackers can carry out illegal activities or acquire private data [99], [100], [105].

3) KEYLOGGERS

Malicious software that records your keystrokes is called a keylogger. Your username, password, and other private information that you type into your computer will all be recorded by the keylogger. There are several ways that keyloggers can get onto your computer: via opening a compromised attachment, clicking on a malicious link, or downloading a file from an untrusted source. Once installed on your computer, a keylogger can give the hacker access to your data [54], [88].

4) SOCIAL ENGINEERING

Social engineering is the practice of coercing someone into disclosing private information or taking activities that compromise the security of their online bank accounts. Attackers fool users by using strategies like urgency, impersonation, and trust-building [92], [106].

5) PHISHING ATTACKS

Phishing attacks are a form of social engineering in which the attackers attempt to get confidential data from the target, such as financial information or login credentials. Usually, this is accomplished by using phoney emails, texts, or websites that impersonate reputable websites. Once a user gives personal information, the attacker can exploit it to access that user's online banking account without authorization [86], [107].

6) MiTM ATTACKS

An attacker performs a MiTM attack by listening to conversations between the user and the online banking system. This enables the attacker to gather private information that may be utilized for fraud or unauthorized access, such as login credentials or financial information [96], [97].

7) DoS ATTACKS

DoS attacks block genuine users from accessing online banking systems by flooding the system with excessive traffic or requests. Services may be interrupted, users may experience inconvenience, and there may be a chance for more security breaches [95], [108], [109].

8) WEAK PASSWORDS

Because they are simple to guess or crack, weak passwords put online banking security at risk. Due to this, they can more easily breach sensitive data, access user accounts without authorization, and engage in fraudulent activity [8], [96].

9) SQL INJECTION

In a SQL injection attack, malicious code is inserted into strings before being sent to a SQL database for execution. Users' credentials, such as usernames and passwords, can be taken by using SQL injection. This can then be used to access user accounts without authorization [110], [111].

10) REPLAY ATTACK

Replay attacks are a type of MiTM attack where an attacker captures a legitimate authentication request and resends it later. This can be done to gain unauthorized access to an online banking account [112], [113], [114].

Knowing that the above attacks could target the supply chain & third-party or endpoint of online banking systems, supply chain attacks occur when attackers gain access to systems through external sources, such as third-party software or vendors [101]. Hackers exploit vulnerabilities in these systems to compromise online banking security, potentially leading to data breaches or unauthorized access. Additionally, endpoint attacks specifically target the user's device or endpoint. Attackers aim to gain access to sensitive banking information stored on the user's device, potentially leading to financial fraud or unauthorized transactions [74].

Table 6, Summarizes the above threats and provides the potential countermeasures that could be applied to prevent them:

Implementing the controls mentioned in the above table is essential for financial institutions to protect their online banking systems and ensure users' financial information security. By adopting a comprehensive approach that includes technological measures (e.g., firewall, antivirus), user education (e.g., awareness, training), policies (e.g., security & privacy policies, password policy) and continuous monitoring, financial institutions can mitigate threats and create a more secure online banking environment.

TABLE 4. User authentication methods of online banking.

Ref.	Method Name	Weaknesses	Strengths
[38], [59], [74], [81], [82]	Passwords	Passwords can be vulnerable to attacks such as: – Brute force attacks – Phishing attacks – Social engineering attacks	– Easy to use and understand. – Can be changed frequently to maintain security. – Relatively inexpensive to implement and maintain. – Can be used as a factor of a 2FA or MFA system.
[43], [46], [50], [83]	PIN	It can be easily guessed. Also, the PIN can be vulnerable to attacks such as: – Brute force attacks – Phishing attacks – Social engineering attacks	– Easy to remember and use. – It can be part of an MFA system.
[66]	Graphical password	Requires users to have a good visual memory.	– It can be easier to remember than traditional passwords. – it can be more resistant to guessing attacks.
[10], [49], [66], [84]	Physiological Biometrics (i.e., Fingerprint, face ID)	– BBA implementation can be complex and may not be suitable for many users. – Concerns about the security and privacy of stored data are brought up using biometric data. – When adopting biometric authentication, factors like user acceptability and hardware requirements need to be taken into consideration.	– It provides a very high level of security and is difficult for attackers to bypass.
[63]	QR Code	– It can be easily copied or stolen. – Requires an additional device to scan it(e.g., smartphone) – Can be affected by environmental factors (e.g., lighting)	– Easy to use, Fast, cheap. – Can provide an extra layer of security when used as a second-factor authentication.
[36], [64]	OTP	– Less convenient than other methods – Can be intercepted by attackers. – depends on the coverage of the phone network	– It provides an extra layer of security and makes it harder for attackers to access user accounts.
[51], [60], [83], [85], [86]	Behavioral Authentication (e.g., Voice pattern, Keystroke)	– It might not work for all users, and it might not be simple to implement. – Over time, changes in user behavior may also have an impact. – Data security and privacy are issues that are brought up using biometric data.	– Behavioral biometrics methods provide several advantages, including being continuous, transparent to the user, and non-intrusive. – It is also challenging for attackers to mimic the habits of trustworthy users.
[31]	OffPAD	– Availability and adoption of offPADs may vary. – Users need access to such devices to benefit from this authentication method. – OffPAD is typically a small, portable device that can be easily lost or stolen.	– It provides an additional layer of security by keeping the authentication process isolated from online threats.
[87], [88]	Challenge questions	– Answers can be guessed or stolen.	– It provides an extra layer of security and makes it harder for attackers to access user accounts.
[69]	MAC addresses	– It can be spoofed.	– Unique to each device. It can be used to track a user's location.
[45]	IMEI numbers	– It can be spoofed.	– Unique to each device.
[43], [71]	IP address	– It can be spoofed.	– It can be used to track a user's location.
[43]	CAPTCHA	– Can be bypassed with advanced algorithms or Optical Character Recognition (OCR)* technology.	– It can be effective at preventing bots from accessing a website.
[70]	Geolocation	– Accuracy can vary, and location can be masked or falsified.	– Adds an extra layer of location-based security.
[48]	Image Recognition	– Image-based authentication can be susceptible to spoofing attacks, where an attacker uses a photo of the user to impersonate them. – It relies on the security of the image database and the potential vulnerability of images being copied or stolen.	– It can be convenient for users.
[10], [41], [46], [49], [50], [89]	2FA & MFA	– It can be time-consuming and inconvenient for users.	– It provides an extra layer of security and makes it harder for attackers to access user accounts.

* OCR stands for Optical Character Recognition. It is a technology that enables the recognition and extraction of text from images or scanned documents.

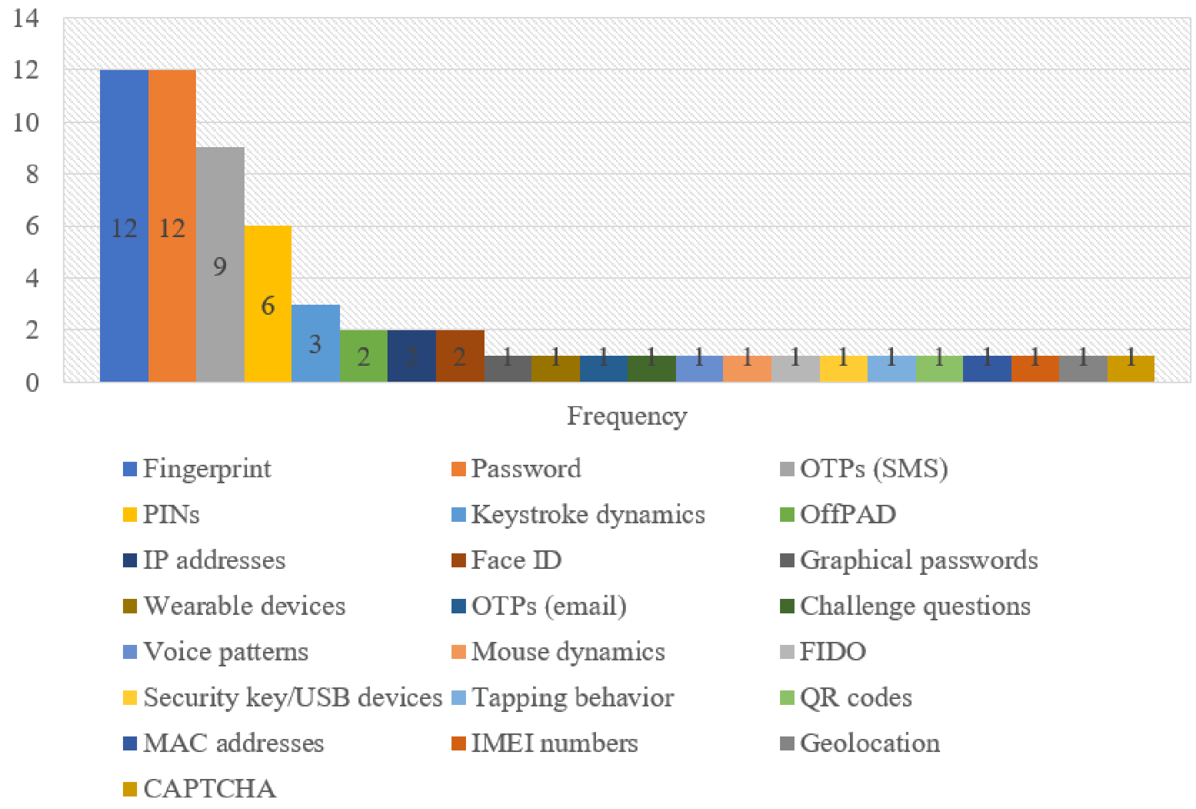

FIGURE 3. Frequency of authentication methods in MFA and 2FA contexts.

C. OVERVIEW OF USER AUTHENTICATION METHODS IN LEADING BANKS

This subsection answers RQ3: "*What are current user authentication methods used by well-known banks worldwide?*". Studying user authentication methods employed by global banks holds significant importance in understanding the evolving landscape of online banking security. The user authentication methods employed by selected banks are summarized in Table 7. The table illustrates the different methods of authentication that banks use to guarantee secure access to their online banking platforms.

The information in Table 7 reveals the user authentication strategies used by several well-known financial institutions, including HSBC Holdings plc, CIMB Bank, Bank of America, Bank of China (BOC), JPMorgan Chase & Co., Citigroup Inc., Barclays plc, and Arab bank. These financial institutions use various authentication techniques because they value keeping their customers' online accounts secure. One of the common authentication methods used by these banks is the password. Customers must create strong passwords that follow specific standards (e.g., NIST password policy), such as being at least eight characters long and combining uppercase and lowercase letters, numbers, and symbols. A crucial security measure is using passwords, which act as the first layer of defense against unauthorized access. One-time password (OTP) authentication is another type of security that many banks employ. Clients who sign in using a new device are sent a unique OTP password via SMS or email. This code must be input to increase further security to complete the login procedure. Because a one-time password is only suitable for one login session and has a short validity period, there is little chance it will be intercepted or used again. As previously mentioned, physiological biometric identification is becoming increasingly popular among banks as a more secure alternative to passwords. Customers' identities are verified using this technology, which uses distinctive physical traits like fingerprints and facial recognition. It is difficult to impersonate vital data, which makes it an effective way to prevent unauthorized access. These banks frequently employ 2FA as a security measure. When logging in from a new device, users must supply a second security factor besides their passwords, such as an OTP or biometric information. Due to the additional layer of security provided by 2FA, it is far more challenging for attackers to access consumer accounts without authorization. Some banks also provide other authentication options such as USB security keys, security questions, challenge/response, voiceprint authentication, and device fingerprints. Device fingerprints help identify which devices have been used by the user, whereas voiceprint authentication employs the unique characteristics of a person's voice. Entering a code produced by the bank and transmitted to the customer's

TABLE 5. User authentication methods used by authors.

References	[35]	[30]	[31]	[32]	[33]	[42]	[38]	[50]	[43]	[44]	[45]	[59]	[36]	[39]	[71]	[65]	[51]	[86]	[47]	[84]	[64]	[90]	[74]	[66]	[91]	[40]	[48]	[46]
Authentication methods/classification	PBA	2FA	2FA	MFA	KBA	MFA	MFA	MFA	MFA	BBA	2FA	MFA	2FA	2FA	MFA	2FA	2FA	2FA	2FA	MFA	2FA	MFA	2FA	MFA	2FA	2FA	2FA	MFA
Password		X		X	X		X		X			X			X	X		X	X		X	X						
Graphical password																								X				
OTP (SMS)				X			X	X					X								X	X		X		X	X	
OTP (Email)															X													
PIN								X	X				X				X			X								X
Fingerprint			X	X		X	X		X			X								X		X	X		X	X		X
Challenge Questions					X																							
Face ID																				X								X
Voice pattern																	X											
Keystroke dynamic														X				X	X									
Mouse dynamic														X														
FIDO						X																						
Security/ USB key						X										X												
Wearable devices	X																						X					
OffPAD			X																						X			
Tapping behavior										X																		
QR code		X																										
MAC addresses											X																	
IP addresses									X						X													
IMEI numbers											X																	
Geolocation															X													
Image Recognition									X																		X	
CAPTCHA								X																				

mobile device is required for the challenge/response. When used in online banking to raise limitations for specific sorts of transfers, a USB security key functions as an additional layer of security and plugs into the USB port on your computer. Customers are prompted to respond to pre-selected questions as part of the login process to add an extra layer of authentication known as security questions. It should be noted that these banks regularly review and update their security measures to stay ahead of emerging threats and protect their customers' accounts. They also provide educational resources to help customers understand the importance of security and how to protect themselves from fraud.

V. CHALLENGES FACING ONLINE BANKING USER AUTHENTICATION

The future of online banking user authentication techniques and cyber threats is unclear, but the stakes are enormous [123]. Financial institutions can protect their consumers and ensure the continuous expansion of online banking by staying on top of the most recent trends. By addressing these challenges, financial institutions can help ensure online banking systems' security in the years to come. The following are some challenges that should be considered to improve the security and user authentication process of online banking systems:

A. QUANTUM COMPUTING CHALLENGE

User authentication for online banking relies heavily on cryptography. To prevent user credentials, such as usernames and passwords, from being intercepted (MiTM Attacks) or taken by cyber-attackers, cryptography is utilized. Additionally, transactions and users are authenticated using cryptography to make sure that only authorized users have access to their accounts and that all transactions are legitimate [124]. Examples of encryption techniques used today by banks to protect the user credential while transmitted and stored include public key encryption algorithms (i.e., asymmetric cryptography) such as RSA (Rivest-Shamir-Adleman), Diffie-Hellman and ECC (Elliptic Curve Cryptography) and symmetric encryption algorithms such as AES (Advanced Encryption Standard). These algorithms are considered very secure, and it will take a very long time to break them using today's computing capabilities [125]. However, the emergence of quantum poses a serious risk to user authentication for online banking. The term ''quantum'' refers to the use of quantum computers, which are technological tools that can carry out calculations based on quantum physics concepts like superposition and entanglement [126]. Some issues could be solved by quantum computers far more quickly than by traditional computers. Many of the current encryption algorithms, particularly those used to safeguard online banking passwords, could be broken by quantum computers [127], [128]. Banks and other financial institutions may utilize post-quantum cryptography to safeguard online banking user authentication against quantum attacks. Post-quantum cryptography refers to a form of cryptographic technique specifically engineered to withstand attacks carried

TABLE 6. Online banking user authentication threats.

Threat	Potential Controls	Ref.
Malwares	• Regularly update and patch systems and applications to fix vulnerabilities. • Implement robust antivirus and anti-malware solutions. • Educate users about safe browsing habits and the importance of not clicking on suspicious links or downloading unknown files.	[85], [96], [99], [100], [108], [109], [119]
Social Engineering	• Educate users about social engineering techniques and common red flags • Implement user awareness programs to promote vigilance and critical thinking. • Establish strict protocols for verifying and authorizing sensitive transactions or requests. .	[111], [120].
Phishing Attacks	• Implement email filtering and spam detection mechanisms. • Train users to recognize phishing attempts and avoid clicking on suspicious links. • Enable two-factor authentication (2FA) to add an extra layer of security.	[91], [112].
Man-in-the-Middle Attacks	• Implement secure communication protocols such as HTTPS. • Utilize encryption techniques to protect data in transit. • Deploy intrusion detection and prevention systems to detect and mitigate man-in-the-middle attacks.	[101], [102].
Denial of Service (DoS) Attacks	• Implement robust network infrastructure with load balancing and traffic management mechanisms. Deploy DoS mitigation solutions to detect and block malicious traffic. • Conduct regular capacity planning and testing to ensure system resilience against DoS attacks.	[100], [113], [116].
Session Hijacking	• Use strong passwords and enable 2FA. • Be cautious of websites and links, and only use secure internet connections. • Keep your software up to date to protect against vulnerabilities. • Watch for signs of session hijacking and contact your bank if you suspect unauthorized access.	[104], [105].
Weak Passwords	• Enforce password complexity requirements and encourage strong, unique passwords. • Implement multi-factor authentication (MFA) to add an extra layer of security. • Regularly educate users about password best practices and the importance of password hygiene.	[119]
Keyloggers	• Use a firewall and antivirus software,be careful about what websites you visit, and Keep your software up to date.	[57], [95].
SQL injection	• Using prepared statements: Prepared statements are a way of preventing SQL injection by preventing users from injecting malicious code into a database. • Sanitizing user input: Sanitizing user input is the process of removing any potentially malicious code from user input before it is processed by a web application. • Keeping software up to date: Keeping software up to date is important because software updates often include security patches that can help to protect against SQL injection attacks.	[115], [116].
Replay attack	• Timestamps can be used to verify the freshness of an authentication request, while nonces are one-time values generated for each authentication request. • Encryption can be used to protect the authentication request from being intercepted by an attacker. • By using these controls together, it is possible to make online banking accounts more secure and resistant to replay attacks.	[?], [35], [118], [121].

out using quantum computers. Post-quantum cryptography is essential in safeguarding user credentials against potential compromise by a cryptanalytically relevant quantum computer (CRQC) [129]. The public-key encryption algorithms now used to protect most digital systems can be broken by CRQCs, which are quantum computers with sufficient processing capacity. A CRQC might seriously compromise sensitive communications, transactions, and infrastructure, which would put many nations' economic and national security at risk. To prevent assaults from either a CRQC or a traditional computer, post-quantum cryptography must be created and put into use. Post-quantum cryptography is a kind of encryption built to withstand quantum attacks. It makes use of mathematical puzzles that are thought to be challenging for quantum computers to solve. A project to standardize post-quantum cryptography was begun by the National Institute of Standards and Technology (NIST) in 2016 to identify and compare the top contenders for post-quantum encryption algorithms. NIST released the first quartet of four algorithms in 2022, marking the beginning of its post-quantum encryption standard. In around two years, the standard should be completed. The standard's objective is to safeguard online banking and other digital services in the future from potential quantum attacks [127], [129]. In addition to using post-quantum cryptography, the MFA method can be used by banks and other financial institutions to reduce the risk of quantum attacks [128]. By implementing post-quantum cryptography, MFA and other quantum-resistant

TABLE 7. User authentication methods employed in selected banks.

Bank Name	Country	User Authentication Methods Used	Ref.
Bank of America	USA	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), Security questions, Device fingerprints, 2FA (Password, OTP).	[122], [123].
Bank of China	China	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), Security questions, USB security keys, Mobile Token (Mobile token app that generates OTPs for customers), 2FA (Password, OTP).	[124]
JPMorgan Chase & Co.	China	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), behavioral biometrics (i.e., Voiceprint authentication), 2FA (Password, OTP).	[125]
Citigroup Inc.	USA	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), Security questions, 2FA (Password, OTP), Challenge/response (Customers can also authenticate their identities using a challenge/response method. This involves entering a code that is generated by the bank and sent to the customer's mobile device).	[122]
HSBC Holdings plc	Hong Kong, multinational banking	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), behavioral biometrics (i.e., Voiceprint authentication), Security questions, 2FA (Password, OTP).	[93]
Barclays plc	UK	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), behavioral biometrics (i.e., Voiceprint authentication), 2FA (Password, OTP).	[93]
Arab bank	Jordan/Middle East	Password, One-time password (OTP), Biometric authentication (fingerprints or facial recognition), 2FA (Password, OTP), Challenge/response.	[126]
CIMB bank	Malaysia/Southeast Asia	Password, One-time password (OTP), Biometric authentication (fingerprints, facial recognition, typing pattern or mouse movements), physical Token, 2FA (Password, OTP).	[127]

technologies, banks and other financial institutions can help protect their customers' accounts and transactions from future quantum attacks.

B. ARTIFICIAL INTELLIGENCE CHALLENGE

Online banking could be put at risk if cyber-attackers employ artificial intelligence (AI), especially machine learning (ML), to breach digital networks or get past detection mechanisms [130], [131], [132], [133]. Several approaches could be utilized to compromise online banking user authentication using ML.

- Deep fakes can be produced, for instance, using ML. Deepfakes are manufactured works of art where the likeness of another person is used to substitute a person in an already-existing photograph or video. When people register into their online banking accounts, phony movies of them doing so might be made using deepfakes, which could then be used to steal their login information [134], [135], [136].
- ML may be used to attack vulnerabilities in authentication systems driven by AI. Though they are still under development, AI-powered authentication solutions are becoming more widespread. AI could be employed to identify and take advantage of these systems' flaws to access users' accounts [133], [137], [138].
- Online banking system attacks could be automated using ML. Attacks on online banking systems, such as guessing attacks, brute-force attacks, and DoS attacks, could be automated with the help of ML techniques. Attackers may find it simpler to mount effective assaults against online banks as a result [133], [139]. Also, Phishing attacks may be launched using ML. Phishing attacks aim to deceive users into disclosing sensitive data like credit card numbers or login credentials. AI might be used to create phishing emails and websites that are more convincing and likely to trick users [140], [141].

However, banks can also utilize ML to strengthen their systems' security and resilience while defending them against cyberattacks. Banks may improve their risk management and compliance procedures as well as detect and stop fraud, malware, phishing, and other risks with the aid of ML. Therefore, depending on how it is applied and managed, ML may both provide a threat and a chance for online banking [142], [143].

C. USER PRIVACY CHALLENGE

User authentication in online banking that relies on BBA (e.g., Fingerprint) is extremely safe and practical because it is considerably more challenging to fake or steal biometric data. BBA, however, is also accompanied by some privacy issues [131], [144]. For instance, if a bank's biometric database is breached, hackers may have access to all of the bank's clientele's biometric information. Some people are also concerned about their biometric data being collected and stored by the banks or other groups [42]. It is the duty of banks using BBA to safeguard the privacy of the biometric information about their clients. This entails taking precautions to shield the data against unlawful use, access, or disclosure. Additionally, banks must have a privacy policy in place that describes to clients how their biometric data will be used.

D. SYSTEM COMPATIBILITY CHALLENGE

Banks may need to modify their current systems and procedures to accommodate the use of a variety of authentication techniques, such as biometrics, Token, MFA, etc., for online banking user authentication. also, if a merchant utilizes third-party payment or billing services, they may need to confirm that these services are appropriate for online banking user authentication and can support the necessary authentication procedures [145], [146].

E. SYSTEM USABILITY CHALLENGE

A well-known problem in the area of user authentication is the trade-off between security and usability. For example, one strategy for improving user authentication security is layering. It entails using several levels of authentication, which may use a variety of authentication techniques, including biometrics, passwords, and security tokens (i.e., MFA). The premise behind layering is that if one layer of security is breached, there will still be other layers of protection in place to keep unauthorized users from accessing the system [4], [73], [147]. So that, layering is that as the number of layers increases, the security of the system improves, but the usability decreases. This is Because the authentication procedure becomes more complex with each new layer, users may become frustrated and confused as a result. On the other side, fewer layers can simplify and improve the usability of the authentication process, but the level of security is also compromised [4]. It is important to balance security and usability, so users need to select authentication methods that are suitable for the necessary security level [12].

VI. CONCLUSION AND FUTURE DIRECTIONS

This research conducted an SLR regarding authentication methods for users in online banks over ten years (2013-2023), where it was found that banks utilize various authentication methods to online banking systems to protect user accounts from unauthorized access. Online banking user authentication methods are divided into four categories: KBA, BBA, PBA, and other methods. Each category includes a variety of authentication methods with varying strengths, weaknesses, and implementation considerations. KBA methods rely on user knowledge, such as passwords, PINs, and security questions, to verify their identity. BBA methods employ unique physiological biometrics (such as fingerprint and face ID) and behavioral biometrics (including voice patterns, keystroke dynamics, and tapping behavior) to confirm users' identities. PBA methods require users to have a token or physical device to access their accounts, such as OTP authentication that generates temporary and exclusive authentication codes delivered through SMS to the user's phone, security keys/USB, OffPAD, and wearable devices. Other methods involve various authentication procedures that do not fit neatly into the KBA, BBA, or PBA categories. Examples include MAC addresses, IMEI numbers, IP addresses, geolocation, CAPTCHAs, FIDO, and QR codes. 2FA and MFA frameworks combine different authentication methods from various categories to significantly improve security. By combining several types of authentication methods, banks can significantly improve the security of their systems and create a layered security approach that is difficult for attackers to crack. This is because if the attacker compromises one layer, the rest of the layers will protect the system. Moreover, The study also covered several cyber threats that can harm online banking systems and explored ways to get over user authentication's protective measures. Among these threats are malware attacks, social engineering, phishing attacks, middleman attacks, denial of service attacks, session hijacking, weak passwords, keyloggers, SQL injection, and replay attacks. In addition, the study explored various well-known banks' methods for user authentication, which can offer insights into the best ways to secure online bank accounts. By discussing the advantages and disadvantages of user authentication methods used in online banking, the research shows that MFA will become increasingly popular in online banking systems for the degree of security it provides to user accounts. The paper also showed that biometric authentication methods, whether physiological or behavioral, will play a large and increasing role in the security of online banking services to the point. The challenges that should be considered to improve the security and user authentication process of online banking systems include quantum computing, AI, privacy, system compatibility, and system usability. A limitation of this paper is that it relied on a literature review of online bank account authentication and did not include digital wallet user authentication and blockchain authentication. Future research should include authentication methods for e-wallets as well as the use of blockchain technology to authenticate users. This paper's findings will interest many stakeholders, including financial institutions, government agencies, and researchers. The findings will help develop new security measures and educational resources to protect online banking users from cyber threats.

CONFLICT OF INTERESTS

The authors declare no conflict of interest.

DATA AVAILABILITY STATEMENT

The data presented in this study are available in the article.

REFERENCES

[1] S. Fox. (2013). *51% of US Adults Bank Online*. Pew Research Center Washington, DC, USA. Accessed: Feb. 24, 2019. [Online]. Available: https://core.ac.uk/download/pdf/71362506.pdf

[2] S. Ahmad, "Demonetization-its impact on banking online transactions," *Sumedha J. Manag.*, vol. 6, no. 3, pp. 4–15, 2017. [Online]. Available: http://search.proquest.com/openview/80b340c087f8285fb81ec91b55e1364a/1?pq-origsite=gscholar&cbl=1936345

[3] H. A. Abdeljaber, "Automatic Arabic short answers scoring using longest common subsequence and Arabic WordNet," *IEEE Access*, vol. 9, pp. 76433–76445, 2021.

[4] N. A. Karim, Z. Shukur, and A. M. Al-Banna, "UIPA: User authentication method based on user interface preferences for account recovery process," *J. Inf. Secur. Appl.*, vol. 52, Jun. 2020, Art. no. 102466.

[5] N. Harini and T. Padmanabhan, "2CAuth: A new two factor authentication scheme using QR-code," *Int. J. Eng. Technol.*, vol. 5, no. 2, pp. 1087–1094, 2013. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.411.9555&rep=rep1&type=pdf

[6] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," *Cryptography*, vol. 2, no. 1, pp. 1–22, Jan. 2018.

[7] N. A. Karim, H. Kanaker, S. Almasadeh, and J. Zarqou, "A robust user authentication technique in online examination," *Int. J. Comput.*, vol. 20, no. 4, pp. 535–542, Dec. 2021.

[8] N. A. Karim and Z. Shukur, "Using preferences as user identification in the online examination," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 6, no. 6, p. 1026, Dec. 2016.

[9] M. K. Normalini and T. Ramayah, "A proposed biometrics technologies implementation in Malaysia internet banking services," in *Proc. 13th Eurasia Bus. Econ. Soc. Conf.*, vol. 1, 2015, pp. 79–87. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-15880-8_7

[10] E. Pakulova, A. Ryndin, and O. Basov, "Multi-path multimodal authentication system for remote information system," in *Proc. 12th Int. Conf. Secur. Inf. Netw.*, Sep. 2019, pp. 1–4, doi: 10.1145/3357613.3357640.

[11] R. D. Silva, "Calls for behavioural biometrics as bank fraud soars," *Biometric Technol. Today*, vol. 2021, no. 9, pp. 7–9, Sep. 2021.

[12] N. A. Karim and Z. Shukur, "Review of user authentication methods in online examination," *Asian J. Inf. Technol.*, vol. 14, no. 5, pp. 166–175, 2015.

[13] 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, Aug. 2020, Art. no. 101745.

[14] O. A. Hassan, A. Samhan, S. Alhajhassan, and R. Hammad, "ARivaT: A tool for automated generation of Riva-based business process architecture diagrams," *IEEE Access*, vol. 11, pp. 46257–46270, 2023.

[15] M. A. Hassan, Z. Shukur, M. K. Hasan, and A. S. Al-Khaleefa, "A review on electronic payments security," *Symmetry*, vol. 12, no. 8, p. 1344, 2020.

[16] Z. Wang and H. Xing, "A kind of rational preference," in *Proc. 9th IEEE Int. Conf. Cognit. Informat. (ICCI)*, Jul. 2010, pp. 754–759.

[17] S. Kiljan, K. Simoens, D. D. E. Cock, M. V. A. N. Eekelen, and H. Vranken, "A survey of authentication and communications security," *ACM Comput.*, vol. 49, no. 4, pp. 1–35, 2016. [Online]. Available: http://dl.acm.org/citation.cfm?id=3002170

[18] C. Wang, Y. Wang, Y. Chen, H. Liu, and J. Liu, "User authentication on mobile devices: Approaches, threats and trends," *Comput. Netw.*, vol. 170, Apr. 2020, Art. no. 107118.

[19] O. M. Ogbanufe and C. Baham, "Using multi-factor authentication for online account security: Examining the influence of anticipated regret," *Inf. Syst. Frontiers*, vol. 25, no. 2, pp. 897–916, Apr. 2022.

[20] N. A. Karim, W. K. Abdulraheem, H. Kanaker, F. I. Alzobi, Z. Shukur, O. Qtaish, and M. Abuhamdeh, "Using interface preferences as evidence of user identity: A feasibility study," *Int. J. Data Netw. Sci.*, vol. 8, no. 1, pp. 537–548, 2024.

[21] N. A. Karim, H. Kanaker, W. K. Abdulraheem, M. A. Ghaith, E. Alhroob, and A. M. F. Alali, "Choosing the right MFA method for online systems: A comparative analysis," *Int. J. Data Netw. Sci.*, vol. 8, no. 1, pp. 201–212, 2024.

[22] S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen, and H. Vranken, "A survey of authentication and communications security in online banking," *ACM Comput. Surv.*, vol. 49, no. 4, pp. 1–35, Dec. 2017.

[23] S. Kiljan, H. Vranken, and M. van Eekelen, "Evaluation of transaction authentication methods for online banking," *Future Gener. Comput. Syst.*, vol. 80, pp. 430–447, Mar. 2018.

[24] W. A. Hammood, R. Abdullah, O. A. Hammood, S. M. Asmara, M. A. Al-Sharafi, and A. M. Hasan, "A review of user authentication model for online banking system based on mobile IMEI number," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 769, no. 1, 2020, Art. no. 012061.

[25] P. Aithal, "A review on advanced security solutions in online banking models," *Int. J. Sci. Res. Modern Educ. (IJSRME)*, vol. 1, pp. 421–429, Jun. 2016.

[26] S. W. Shah and S. S. Kanhere, "Recent trends in user authentication—A survey," *IEEE Access*, vol. 7, pp. 112505–112519, 2019.

[27] S. Keele. (2007). *Guidelines for Performing Systematic Literature Reviews in Software Engineering*. [Online]. Available: http://www.academia.edu/download/35830450/2_143465389588742151.pdf

[28] K. Takatori, "Mendeley; Reference manager," *Kyokai Joho Imeji Zasshi/J. Inst. Image Inf. Telev. Eng.*, vol. 70, pp. 320–323, 2016.

[29] S. Shamal, K. Monika, and N. Neha, "Secure authentication for online banking using QR code," *IJETAE-Int. J. Emerg. Technol. Advance Eng.*, Mar. 2014.

[30] A. Plateaux, P. Lacharme, A. Jøsang, and C. Rosenberger. (2014). *One-Time Biometrics for Online Banking Electron, Payment Authentication*. [Online]. Available: http://link.springer.com/10.1007/978-3-319-10975-6_14

[31] S. Nagaraju and L. Parthiban, "Trusted framework for online banking in public cloud using multi-factor authentication and privacy protection gateway," *J. Cloud Comput.*, vol. 4, no. 1, p. 22, Dec. 2015. [Online]. Available: http://www.journalofcloudcomputing.com/content/4/1/22

[32] P. C. Mondal, R. Deb, and M. N. Huda, "Transaction authorization from know your customer (KYC) information in online banking," in *Proc. 9th Int. Conf. Elect. Comput. Eng.*, 2016, pp. 523–526. [Online]. Available: http://ieeexplore.ieee.org/document/7853972/

[33] B. Akoramurthy and J. Arthi, "GeoMoB—A geo location based browser for secured mobile banking," in *Proc. 8th Int. Conf. Adv. Comput. (ICoAC)*, Jan. 2017, pp. 83–88.

[34] A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, "A secure and practical authentication scheme using personal devices," *IEEE Access*, vol. 5, pp. 11677–11687, 2017. [Online]. Available: http://ieeexplore.ieee.org/document/7954590/

[35] A. Sheshasaayee and D. Sumathy, "A framework to enhance security for OTP SMS in e-banking environment using cryptography and text steganography," in *Proc. Int. Conf. Data Eng. Commun. Technol.*, vol. 469, 2017, pp. 709–717.

[36] B. K. Alese, A. F.-B. Thompson, O. D. Alowolodu, and B. E. Oladele, "Multilevel authentication system for stemming crime in online banking," *Interdiscipl. J. Inf., Knowl., Manag.*, vol. 13, pp. 79–94, Jan. 2018. [Online]. Available: http://www.ijikm.org/Volume13/IJIKMv13p079-094Alese4509.pdf

[37] M. Bartlomiejczyk, E. F. Imed, and M. Kurkowski, "Multifactor authentication protocol in a mobile environment," *IEEE Access*, vol. 7, pp. 157185–157199, 2019.

[38] K. Chatterjee, "Continuous user authentication system: A risk analysis based approach," *Wireless Pers. Commun.*, vol. 108, no. 1, pp. 281–295, Sep. 2019.

[39] A. T. Kiyani, A. Lasebae, K. Ali, and M. Ur-Rehman, "Secure online banking with biometrics," in *Proc. Int. Conf. Adv. Emerg. Comput. Technol. (AECT)*, Feb. 2020, pp. 1–6. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/9194214/

[40] Z. P. Zwane, T. E. Mathonsi, and S. P. Maswikaneng, "An intelligent security model for online banking authentication," in *Proc. IST-Africa Conf.*, 2021, pp. 1–6.

[41] G. L. Moepi and T. E. Mathonsi, "Multi-factor authentication method for online banking services in South Africa," in *Proc. Int. Conf. Elect., Comput. Energy Technol.*, 2021, pp. 1–5.

[42] S. L. Sahdev, S. Singh, N. Kaur, and L. Siddiqui, "Behavioral biometrics for adaptive authentication in digital banking—Guard against flawless privacy," in *Proc. Int. Conf. Innov. Practices Technol. Manag.*, 2021, pp. 261–265.

[43] W. A. Hammood, R. A. Arshah, S. M. Asmara, and O. A. Hammood, "User authentication model based on mobile phone IMEI number: A proposed method application for online banking system," in *Proc. Int. Conf. Softw. Eng. Comput. Syst. 4th Int. Conf. Comput. Sci. Inf. Manag. (ICSECS-ICOCSIM)*, Aug. 2021, pp. 411–416.

[44] C. U. Bah, A. H. Seyal, and U. Yahya, "Combining pin and biometric identifications as enhancement to user authentication in internet banking," in *Proc. 7th Brunei Int. Conf. Eng. Technol.*, 2021, pp. 1—8.

[45] F. Pirzado, S. Memon, L. D. D. Dhomeja, and A. Ahmed, "Keystroke dynamics based technique to enhance the security in smart devices," *KIET J. Comput. Inf. Sci.*, vol. 4, no. 1, p. 14, Jan. 2021.

[46] A. Ara, A. Sharma, and D. Yadav, "An efficient privacy-preserving user authentication scheme using image processing and blockchain technologies," *J. Discrete Math. Sci. Cryptography*, vol. 25, no. 4, pp. 1137–1155, May 2022.

[47] S. Hublikar, V. B. Pattanashetty, V. Mane, P. S. Pillai, M. Lakkannavar, and N. S. Shet, "Biometric-based authentication in online banking," in *Information and Communication Technology for Competitive Strategies* (Lecture Notes in Networks and Systems), vol. 400. Singapore: Springer, 2023, pp. 249–259, doi: 10.1007/978-981-19-0095-2_26.

[48] M. K. Abiodun, J. B. Awotunde, A. E. Adeniyi, D. Ademuagun, and D. R. Aremu, "Securing digital transaction using a three-level authentication system," in *Computational Science and Its Applications—ICCSA* (Lecture Notes in Computer Science), vol. 13380. Springer, 2022, pp. 135–148, doi: 10.1007/978-3-031-10542-5_10.

[49] A. Renz, T. Neff, M. Baldauf, and E. Maier, "Authentication methods for voice services on smart speakers—A multi-method study on perceived security and ease of use," *I-COM*, vol. 22, pp. 67–81, Apr. 2023. [Online]. Available: https://www.degruyter.com/document/doi/10.1515/icom-2022-0039/html

[50] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, ISO/IEC 27002 AND PCI DSS," *Int. J. Inform. Vis.*, vol. 4, no. 4, pp. 225–230, 2020.

[51] S. Jarecki, M. Jubur, H. Krawczyk, N. Saxena, and M. Shirvanian, "Two-factor password-authenticated key exchange with end-to-end security," *ACM Trans. Privacy Secur.*, vol. 24, no. 3, pp. 1–37, Aug. 2021.

[52] B. Bhana and S. Flowerday, "Passphrase and keystroke dynamics authentication: Usable security," *Comput. Secur.*, vol. 96, Sep. 2020, Art. no. 101925.

[53] Y. S. Chuen, M. Al-Rashdan, and Q. Al-Maatouk, "Graphical password strategy," *J. Crit. Rev.*, vol. 7, pp. 102–104, Jan. 2020.

[54] M. Verma, R. Sawhney, and R. Chalia, "Biometric based user authentication in smart phones," in *Proc. Int. Conf. Next Gener. Comput. Inf. Syst. (ICNGCIS)*, Dec. 2017, pp. 183–188.

[55] A. G. Johansen, "Biometrics and biometric data: What is it and is it secure?" IEEE, Tech. Rep., 2019.

[56] V. Jancok and M. Ries, "Security aspects of behavioral biometrics for strong user authentication," in *Proc. Int. Conf. Comput. Syst. Technol.*, Jun. 2022, pp. 57–63. [Online]. Available: https://dl.acm.org/doi/10.1145/3546118.3546152

[57] M. Stokkenes, R. Ramachandra, and C. Busch, "Biometric transaction authentication using smartphones," in *Proc. Int. Conf. Biometrics Special Interest Group (BIOSIG)*, Sep. 2018, pp. 1–5.

[58] A. Sarkar and B. K. Singh, "A review on performance, security and various biometric template protection schemes for biometric authentication systems," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 27721–27776, Oct. 2020.

[59] Y. W. Chow, W. Susilo, G. Yang, M. H. Au, and C. Wang, "Authentication and transaction verification using QR codes with a mobile device," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage* (Lecture Notes in Computer Science), vol. 10066. Zhangjiajie, China: Springer, 2016, pp. 437–451, doi: 10.1007/978-3-319-49148-6_36.

[60] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "OTP-based two-factor authentication using mobile phones," in *Proc. 8th Int. Conf. Inf. Technol., New Gener.*, 2011, pp. 327–331.

[61] E. O. Vinbæk, F. M. B. Pettersen, J. E. Carlsen, K. Fremstad, N. Edvinsen, and F. E. Sandnes, "On online banking authentication for all: A comparison of bankid login efficiency using smartphones versus code generators," in *Proc. Int. Conf. Human-Comput. Interact.*, vol. 11572, 2019, pp. 365–374.

[62] P. Nandi and D. P. Savant, "Graphical password authentication system," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 10, no. 4, pp. 1759–1765, Apr. 2022.

[63] M. Alhaidary, S. M. M. Rahman, M. Zakariah, M. S. Hossain, A. Alamri, M. S. M. Haque, and B. B. Gupta, "Vulnerability analysis for the authentication protocols in trusted computing platforms and a proposed enhancement of the OffPAD protocol," *IEEE Access*, vol. 6, pp. 6071–6081, 2018.

[64] M. E. Farfoura, O. A. Khashan, H. Omar, Y. Alshamaila, N. A. Karim, H.-T. Tseng, and M. Alshinwan, "A fragile watermarking method for content-authentication of H. 264-AVC video," *J. Internet Services Inf. Secur.*, vol. 13, no. 2, pp. 211–232, 2023. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85162828477&doi=10.58346%2fJISIS.2023.I2.014&partnerID=40&md5=849a4d9a7175429406e4d7963b3ea966, doi: 10.58346/JISIS.2023.I2.014.

[65] M. A. Hassan and Z. Shukur, "Device identity-based user authentication on electronic payment system for secure E-wallet apps," *Electronics*, vol. 11, no. 1, p. 4, Dec. 2021.

[66] N. Akhtar and F. U. Haq, "Real time online banking fraud detection using location information," in *Proc. Int. Conf. Comput. Intell. Inf. Technol.*, vol. 250, 2011, pp. 770–772, doi: 10.1007/978-3-642-25734-6_136.

[67] K. R. J. Joshi. (2016). *Security Analysis and Comparison of Nepalese Internet Banking Web Applications*. [Online]. Available: https://elibrary.tucl.edu.np/handle/123456789/7902

[68] M. Hijjawi, M. A. Shinwan, M. H. Qutqut, W. Alomoush, O. A. Khashan, M. Alshdaifat, A. Alsokkar, and L. Abualigah, "Improved flat mobile core network architecture for 5G mobile communication systems," *Int. J. Data Netw. Sci.*, vol. 7, no. 3, pp. 1421–1434, 2023.

[69] N. Kheshaifaty and A. Gutub, "Engineering graphical captcha and AES crypto hash functions for secure online authentication," *J. Eng. Res.*, Nov. 2021. [Online]. Available: https://kuwaitjournals.org/jer/index.php/JER/article/view/13761

[70] K. Wong and M. H. Kim, "An enhanced user authentication solution for mobile payment systems using wearables," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4639–4649, Nov. 2016.

[71] L. Zhang. (2018). *Smartphone App Security: Vulnerabilities and Implementations*. [Online]. Available: https://deepblue.lib.umich.edu/handle/2027.42/143522

[72] S. Sciancalepore, S. Raponi, D. Caldarola, and R. D. Pietro, "Fractal: Single-channel multi-factor transaction authentication through a compromised terminal," in *Information and Communications Security* (Lecture Notes in Computer Science), vol. 13407. Springer, 2022, pp. 201–217, doi: 10.1007/978-3-031-15777-6_12.

[73] D. Cherry, "Multi-factor authentication," in *Enterprise-Grade IT Security for Small and Medium Businesses: Building Security Systems, in Plain English*. Berkeley, CA, USA: Apress, 2022, pp. 83–96, doi: 10.1007/978-1-4842-8628-9_7.

[74] A. Q. Stanikzai and M. A. Shah, "Evaluation of cyber security threats in banking systems," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2021, pp. 1–4.

[75] K. Malinka, O. Hujnák, P. Hanácek, and L. Hellebrandt, "E-banking security study—10 years later," *IEEE Access*, vol. 10, pp. 16681–16699, 2022.

[76] M. Alshinwan, A. Y. Shdefat, N. Mostafa, A. A. M. AlSokkar, T. Alsarhan, and D. Almajali, "Integrated cloud computing and blockchain systems: A review," *Int. J. Data Netw. Sci.*, vol. 7, no. 2, pp. 941–956, 2023.

[77] D. Choi, D. Tak, and I. Chung, "Secure password-based authentication method for mobile banking services," *J. Korea Multimedia Soc.*, vol. 19, no. 1, pp. 41–50, Jan. 2016.

[78] M. A. Hassan, Z. Shukur, and M. K. Hasan, "Electronic wallet payment system in Malaysia," *Lect. Notes Data Eng. Commun. Technol.*, vol. 54, pp. 711–736, 2021.

[79] A. Renz, M. Baldauf, E. Maier, and F. Alt, "Alexa, it's me! An online survey on the user experience of smart speaker authentication," in *Proc. ACM Int. Conf.*, vol. 22, 2022, pp. 14–24, doi: 10.1145/3543758.3543765.

[80] R. Batie Jr., Y. Levy, S. Furnell, and P. Liu, "Improving user authentication with fingerprint biometrics and biometric personal identification number (BIO-PINTM) as a multi-factor authentication mechanism," Tech. Rep., 2015.

[81] S. K. A. Kumar, G. V. Ihita, S. Chaudhari, and P. Arumugam, "A survey on rural internet connectivity in India," in *Proc. 14th Int. Conf. Commun. Syst. Netw.*, 2022, pp. 911–916.

[82] F. Ebbers and P. Brune, "The authentication game—Secure user authentication by gamification?" in *Proc. Int. Conf. Adv. Inf. Syst. Eng.*, vol. 9694, 2016, pp. 101–115.

[83] R. AlHusain and A. Alkhalifah, "Evaluating fallback authentication research: A systematic literature review," *Comput. Secur.*, vol. 111, Dec. 2021, Art. no. 102487.

[84] K. Skracic, P. Pale, and B. Jeren, "Question based user authentication in commercial environments," in *Proc. 37th Int. Conv. Inf. Commun. Technol., Electron. Microelectron. (MIPRO)*, May 2014, pp. 1422–1427.

[85] A. D. Rubin, "Taking two-factor to the next level: Protecting online poker, banking, healthcare and other applications," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 1–5, doi: 10.1145/2664243.2684461.

[86] D. Migdal, C. Johansen, and A. Jøsang, "DEMO: OffPAD-offline personal authenticating device with applications in hospitals and e-banking," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 1847–1849, doi: 10.1145/2976749.2989033.

[87] X. Wang, Z. Yan, R. Zhang, and P. Zhang, "Attacks and defenses in user authentication systems: A survey," *J. Netw. Comput. Appl.*, vol. 188, Aug. 2021, Art. no. 103080.

[88] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, "Online authentication methods used in banks and attacks against these methods," *Proc. Comput. Sci.*, vol. 151, pp. 1052–1059, Jan. 2019.

[89] C. Yoo, B.-T. Kang, and H. K. Kim, "Case study of the vulnerability of OTP implemented in internet banking systems of South Korea," *Multimedia Tools Appl.*, vol. 74, no. 10, pp. 3289–3303, May 2015, doi: 10.1007/s11042-014-1888-3.

[90] I. Oh, K. Lee, S. Y. Lee, K. Do, H. B. Ahn, and K. Yim, "Vulnerability analysis on the image-based authentication through the PS/2 interface," in *Proc. Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput.* (Advances in Intelligent Systems and Computing), vol. 773, 2019, pp. 212–219, doi: 10.1007/978-3-319-93554-6_19.

[91] A. Rawat, A. K. Singh, J. Jithin, N. Jeyanthi, and R. Thandeeswaran, "RSJ approach for user authentication," in *Proc. Int. Conf. Adv. Inf. Commun. Technol. Comput.*, vol. 12, 2016, pp. 1–6, doi: 10.1145/2979779.2979880.

[92] J. Banerjee, D. Majumdar, M. S. Pal, and D. Majumdar, "Readability, subjective preference and mental workload studies on Young Indian adults for selection of optimum font type and size during onscreen reading," *Al Ameen J. Med. Sci.*, vol. 4, pp. 131–143, Jan. 2011. [Online]. Available: http://ezproxy.lib.utexas.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=59806916&site=ehost-live

[93] M. A. H. Sijan, A. Shahoriar, M. Salimullah, A. S. Islam, and R. H. Khan, "A review on E-banking security in Bangladesh: An empirical study," in *Proc. 2nd Int. Conf. Comput. Advancements*, Mar. 2022, pp. 330–336, doi: 10.1145/3542954.3543002.

[94] M. Botacin, H. Aghakhani, S. Ortolani, C. Kruegel, G. Vigna, D. Oliveira, P. L. D. Geus, and A. Grégio, "One size does not fit all," *ACM Trans. Privacy Secur. (TOPS)*, vol. 24, pp. 1–31, Jan. 2021, doi: 10.1145/3429741.

[95] Z. T. Mamadiyarov, "Risk management in the remote provision of banking services in the conditions of digital transformation of banks," in *Proc. 5th Int. Conf. Future Netw. Distrib. Syst.*, Dec. 2021, pp. 311–317, doi: 10.1145/3508072.3508119.

[96] K. Kaushik, V. Singh, and V. P. Manikandan, "A novel approach for an automated advanced MITM attack on IoT networks," in *Proc. Int. Conf. Advancements Interdiscipl. Res.*, vol. 1738, 2022, pp. 60–71.

[97] S. Yu and Y. Park, "ITSSAKA-MS: An improved three-factor symmetric-key based secure AKA scheme for multi-server environments," *IEEE Access*, vol. 8, pp. 193375–193379, 2020.

[98] F. S. D. Lima Filho, F. A. F. Silveira, A. de M. B. Junior, G. Vargas-Solar, and L. F. Silveira, "Smart detection: An online approach for DoS/DDoS attack detection using machine learning," *Secur. Commun. Netw.*, vol. 2019, pp. 1–15, Oct. 2019.

[99] R. Singh and A. Soumya, "Updated comparative analysis on video conferencing platforms-zoom, Google meet, Microsoft Teams, WebEx Teams and GoToMeetings," *EasyChair, World Scientists*, vol. 4026, pp. 1–9, Aug. 2020.

[100] P. Shrestha and N. Saxena, "Hacksaw: Biometric-free non-stop web authentication in an emerging world of wearables," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2020, pp. 13–24.

[101] M. Ohm, H. Plate, A. Sykosch, and M. Meier, "Backstabber's knife collection: A review of open source software supply chain attacks," in *Detection of Intrusions and Malware, and Vulnerability Assessment* (Lecture Notes in Computer Science), vol. 12223. Heidelberg, Germany: Springer, 2020, pp. 23–43, doi: 10.1007/978-3-030-52683-2_2.

[102] O. Jullian, B. Otero, E. Rodriguez, N. Gutierrez, H. Antona, and R. Canal, "Deep-learning based detection for cyber-attacks in IoT networks: A distributed attack detection framework," *J. Netw. Syst. Manag.*, vol. 31, no. 2, p. 33, Apr. 2023.

[103] M. Alazab, "A discrete time-varying greywolf IoT botnet detection system," *Comput. Commun.*, vol. 192, pp. 405–416, Aug. 2022.

[104] M. Alazab, R. A. Khurma, A. Awajan, and D. Camacho, "A new intrusion detection system based on moth-flame optimizer algorithm," *Exp. Syst. Appl.*, vol. 210, Dec. 2022, Art. no. 118439.

[105] M. Hijjawi, M. Alshinwan, O. A. Khashan, W. Alomoush, N. A. Karim, A. Y. Shdefat, S. S. Alqahtany, and E. Shudayfat, "A novel hybrid Prairie dog algorithm and Harris hawks algorithm for resource allocation of wireless networks," *IEEE Access*, early access.

[106] H. Chen, F. Li, W. Du, S. Yang, M. Conn, and Y. Wang, "Listen to your fingers: User authentication based on geometry biometrics of touch gesture," *Proc. ACM Interact., Mobile, Wearable Ubiquitous Technol.*, vol. 4, pp. 1–23, Sep. 2020, doi: 10.1145/3411809.

[107] S. Manoharan, N. Katuk, S. Hassan, and R. Ahmad, "To click or not to click the link: The factors influencing internet banking users' intention in responding to phishing emails," *Inf. Comput. Secur.*, vol. 30, pp. 37–62, Jan. 2022.

[108] M. Shurman, R. Khrais, and A. Yateem, "DoS and DDoS attack detection using deep learning and IDS," *Int. Arab J. Inf. Technol.*, vol. 17, no. 4, pp. 655–661, Jul. 2020.

[109] D. Barik, J. Sanyal, and T. Samanta, "Denial-of-Service attack mitigation in multi-hop 5G D2D wireless communication networks employing double auction game," *J. Netw. Syst. Manag.*, vol. 31, no. 1, pp. 1–30, Jan. 2023, doi: 10.1007/s10922-022-09695-z.

[110] P. Revathy and G. B. Jebamalar, *A Review Based on Secure Banking Application Against Server Attacks*, vol. 38. IOS Press, 2021.

[111] K. B. Jalbani, M. Yousaf, M. S. Sarfraz, R. J. Oskouei, A. Hussain, and Z. Memon, "Poor coding leads to DoS attack and security issues in web applications for sensors," *Secur. Commun. Netw.*, vol. 2021, pp. 1–11, May 2021.

[112] A. Kaur and K. Mustafa, "Preference-oriented password-based authentication," in *Information and Communication Technology for Competitive Strategies* (Lecture Notes in Networks and Systems), vol. 191. Singapore: Springer, 2022, pp. 953–965.

[113] L. Li, Z. Xia, J. Wu, L. Yang, and H. Han, "Face presentation attack detection based on optical flow and texture analysis," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1455–1467, Apr. 2022.

[114] R. H. Khan and J. Miah, "Performance evaluation of a new one-time password (OTP) scheme using stochastic Petri net (SPN)," in *Proc. IEEE World AI IoT Congr. (AIIoT)*, Jun. 2022, pp. 407–412.

[115] H. Kanaker, N. A. Karim, S. A. B. Awwad, N. H. A. Ismail, J. Zraqou, and A. M. F. Al Ali, "Trojan horse infection detection in cloud based environment using machine learning," *Int. J. Interact. Mobile Technol. (iJIM)*, vol. 16, no. 24, pp. 81–106, Dec. 2022.

[116] S. Banerjee, M. P. Dutta, and C. T. Bhunia, "A perfect dynamic-id and biometric based remote user authentication scheme under multi-server environments using smart cards," in *Proc. 8th Int. Conf. Secur. Inf. Netw.*, Sep. 2015, pp. 58–64, doi: 10.1145/2799979.2799984.

[117] *FFIEC Home Page*. Accessed: May 1, 2023. [Online]. Available: https://www.ffiec.gov/

[118] *Online Banking Security Features FAQS—Bank of America Security Center*. Accessed: May 15, 2023. [Online]. Available: https://www.bankofamerica.com/security-center/faq/additional-security-features/

[119] *Security Mechanism(Corporate Service)*. Accessed: Aug. 19, 2023. [Online]. Available: https://www.bankofchina.com/en/custserv/bocnet/200812/t20081212_144526.html

[120] *How to Stay a Step Ahead of Fraudsters | JP Morgan Private Bank*. Accessed: Aug. 19, 2023. [Online]. Available: https://privatebank.jpmorgan.com/gl/en/about-us/cybersecurity-and-fraud-prevention-hub/how-to-stay-a-step-ahead-of-fraudsters

[121] *Security Statement*. Accessed: Aug. 19, 2023. [Online]. Available: https://www.arabbank.jo/footernavigation/security-statement

[122] *Branchless Banking Cimb Niaga*. Accessed: Aug. 21, 2023. [Online]. Available: https://branchlessbanking.cimbniaga.co.id/en/gomobiletnc-2/

[123] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: A comprehensive survey," *J. Defense Model. Simul., Appl., Methodol., Technol.*, vol. 19, no. 1, pp. 57–106, Jan. 2022.

[124] D. Sadhukhan, S. Ray, G. P. Biswas, M. K. Khan, and M. Dasgupta, "A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography," *J. Supercomput.*, vol. 77, no. 2, pp. 1114–1151, Feb. 2021.

[125] S. Jagadeesh, S. M. Ali, S. P. G. Selvan, M. Aljanabi, M. Gopianand, and J. P. J. Hephzipah, "Hybrid AES-modified ECC algorithm for improved data security over cloud storage," *J. Adv. Res. Appl. Sci. Eng. Technol.*, vol. 32, no. 1, pp. 46–56, Aug. 2023.

[126] J. L. Hevia, G. Peterssen, C. Ebert, and M. Piattini, "Quantum computing," *IEEE Softw.*, vol. 38, no. 5, pp. 7–15, Sep. 2021.

[127] A. Sharma and S. K. Lenka, "E91 QKD protocol for authentication in online banking systems," *Int. J. Bus. Inf. Syst.*, vol. 22, no. 1, pp. 116–122, 2016.

[128] R. A. Grimes, *Hacking Multifactor Authentication*. Hoboken, NJ, USA: Wiley, 2020.

[129] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A survey of post-quantum cryptography: Start of a new race," *Cryptography*, vol. 7, no. 3, p. 40, Aug. 2023.

[130] S. Biswas, B. Carson, V. Chung, S. Singh, and R. Thomas, *AI-Bank of the Future: Can Banks Meet the AI Challenge*. New York, NY, USA: McKinsey, 2020.

[131] H. U. Khan, M. Z. Malik, S. Nazir, and F. Khan, "Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis," *IEEE Access*, vol. 11, pp. 80181–80198, 2023.

[132] K. Morovat and B. Panda, "A survey of artificial intelligence in cybersecurity," in *Proc. Int. Conf. Comput. Sci. Comput. Intell. (CSCI)*, Dec. 2020, pp. 109–115.

[133] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A survey on machine learning techniques for cyber security in the last decade," *IEEE Access*, vol. 8, pp. 222310–222354, 2020.

[134] C.-Z. Yang, J. Ma, S. Wang, and A. W. Liew, "Preventing DeepFake attacks on speaker authentication by dynamic lip movement analysis," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1841–1854, 2021.

[135] P. Chhajed and D. Phalke, "A review on deepfake attack detection of user," Tech. Rep.

[136] A. Alomari, N. Idris, A. Q. M. Sabri, and I. Alsmadi, "Deep reinforcement and transfer learning for abstractive text summarization: A review," *Comput. Speech Lang.*, vol. 71, Jan. 2022, Art. no. 101276.

[137] Y. Sun and L. Gu, "Attention-based machine learning model for smart contract vulnerability detection," *J. Phys., Conf.*, vol. 1820, no. 1, Mar. 2021, Art. no. 012004.

[138] K. Filus and J. Domanska, "Software vulnerabilities in TensorFlow-based deep learning applications," *Comput. Secur.*, vol. 124, Jan. 2023, Art. no. 102948.

[139] F. Musumeci, A. C. Fidanci, F. Paolucci, F. Cugini, and M. Tornatore, "Machine-learning-enabled DDoS attacks detection in p4 programmable networks," *J. Netw. Syst. Manag.*, vol. 30, no. 1, pp. 1–27, Jan. 2022.

[140] A. C. Bahnsen, I. Torroledo, L. D. Camacho, and S. Villegas, "Deepphish: Simulating malicious ai," in *Proc. APWG Symp. Electron. Crime Res. (eCrime)*, 2018, pp. 1–8.

[141] A. Basit, M. Zafar, X. Liu, A. R. Javed, Z. Jalil, and K. Kifayat, "A comprehensive survey of AI-enabled phishing attacks detection techniques," *Telecommun. Syst.*, vol. 76, no. 1, pp. 139–154, Jan. 2021.

[142] M. Hijjawi, M. Alshinwan, O. A. Khashan, M. Alshdaifat, W. Almanaseer, W. Alomoush, H. Garg, and L. Abualigah, "Accelerated arithmetic optimization algorithm by cuckoo search for solving engineering design problems," *Processes*, vol. 11, no. 5, p. 1380, May 2023.

[143] L. Abualigah, D. Oliva, H. Jia, F. Gul, N. Khodadadi, A. G. Hussien, M. A. Shinwan, A. E. Ezugwu, B. Abuhaija, and R. A. Zitar, "Improved Prairie dog optimization algorithm by dwarf mongoose optimization algorithm for optimization problems," *Multimedia Tools Appl.*, pp. 1–41, Sep. 2023.

[144] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[145] Y. Chandrasekran, C. R. Ramachandiran, and K. C. Arun, "Adoption of future banking using biometric technology in automated teller machine (ATM)," in *Proc. IEEE Int. Conf. Distrib. Comput. Electr. Circuits Electron. (ICDCECE)*, Apr. 2022, pp. 1–4.

[146] P. M. C. Arta, D. Bagus, A. Dodik, and S. H. Bambang, "Factor analysis of the net benefits of accounting information systems with system use and user satisfaction as mediating variables," *Eurasia, Econ. Bus.*, vol. 1, no. 43, pp. 34–48, 2021.

[147] Y. Oren and D. Arad, "Toward usable and accessible two-factor authentication based on the piezo-gyro channel," *IEEE Access*, vol. 10, pp. 19551–19557, 2022.

NADER ABDEL KARIM received the Ph.D. degree in cybersecurity from UKM, in 2017. He is currently a Faculty Member with the Department of Cybersecurity, College of Artificial Intelligence, Al-Balqa Applied University. He is also a Distinguished Cybersecurity Expert. His contributions to the field extend beyond academia, as he actively shares knowledge through prolific writing for specialized websites, such as CyberX. His articles cover a wide range of cybersecurity topics, from in-depth analyses of emerging threats to practical guides for implementing robust security measures. Notably, the work on user authentication methods has garnered attention for striking a balance between security and user convenience. He has a very strong experience in the areas of user authentication, cyber security, human–computer interaction (HCI), and online learning. He has also participated in a number of research projects, including ones on virtual privacy techniques and preferences-based authentication.

OSAMA AHMED KHASHAN received the M.Sc. degree in information technology from Universiti Utara Malaysia, Malaysia, in 2008, and the Ph.D. degree in computer science from the National University of Malaysia, Malaysia, in 2014. He is currently an Associate Professor/Associate Researcher with the Research and Innovation Centers, Rabdan Academy, Abu Dhabi, United Arab Emirates. His research interests include information security, cyber security, cryptography, blockchain technology, the Internet of Things, and image processing.

HASAN KANAKER received the Ph.D. degree from Islamic Science University of Malaysia (USIM), in 2018. He is currently the Head of the Department of Computer Information System and the Department of Cybersecurity, Isra University, Jordan. He has a very strong experience in the areas of networking, malware detection, cyber security, and online education. In addition, he had been working on a number of research projects, including one detection of malware in the cloud computing environment, user authentication for online exams, and utilizing neural networks to analyze medical images. His research interests include network security, intrusion detection, data mining, malware detection, machine learning, cloud computing security, and information security.

WALEED K. ABDULRAHEEM received the B.S. degree in computer and networks from Arab Open University, Jordan, in 2012, the M.S. degree in computer and information security from Middle East University, Jordan, in 2014, and the Ph.D. degree in cybersecurity from Universiti Putra Malaysia, Malaysia, in 2019. He is currently an Assistant Professor with The World Islamic Sciences and Education University. His research interests include cryptography, the IoT security, and cloud security.

MOHAMMAD ALSHINWAN received the Ph.D. degree from the School of Computer Engineering, Inje University, Gimhae, Republic of Korea, in 2017. He was an Assistant Professor with the Department of Computer and Information Sciences, Amman Arab University, Jordan. He is currently an Associate Professor with Applied Science Private University, Jordan. His research interests include computer networks, mobile networks, information security, AI, and optimization methods.

ABEDAL-KAREEM AL-BANNA is currently pursuing the Ph.D. degree with Loughborough University, U.K. He is the CTO and the Co-Founder of Jordanian Startup called TAKALAM, a company that provides solutions for hearing and speech disorders. He is a member of the Leaders in Innovation Fellowship at the Royal Academy of Engineering, U.K., in 2020.

• • •