



USENIX

THE ADVANCED COMPUTING
SYSTEMS ASSOCIATION

SoK: Inaccessible & Insecure: An Exposition of Authentication Challenges Faced by Blind and Visually Impaired Users in State-of-the-Art Academic Proposals

Md Mojibur Rahman Redoy Akanda, Amanda Lacy,
and Nitesh Saxena, *Texas A&M University*

<https://www.usenix.org/conference/usenixsecurity25/presentation/akanda>

**This paper is included in the Proceedings of the
34th USENIX Security Symposium.**

August 13–15, 2025 • Seattle, WA, USA

978-1-939133-52-6

Open access to the Proceedings of the
34th USENIX Security Symposium is sponsored by USENIX.

SoK: Inaccessible & Insecure: An Exposition of Authentication Challenges Faced by Blind and Visually Impaired Users in State-of-the-Art Academic Proposals

Md Mojibur Rahman Redoy Akanda
redoy.akanda@tamu.edu
Texas A&M University

Amanda Lacy
aklacy@tamu.edu
Texas A&M University

Nitesh Saxena
nsaxena@tamu.edu
Texas A&M University

Abstract

Despite the proliferation of advanced authentication methods in the academic research literature, it is not clear whether these methods would be suitable for blind and visually impaired users in terms of accessibility and security. To address this issue, we first developed the *Authentication Literature Evaluation for Security and Accessibility (ALESA)* framework consisting of 5 accessibility and 8 security features to measure the accessibility and security of these methods. Then, using this framework, we systematically evaluated 37 selected general-purpose academic authentication schemes if they were to be used by blind and visually impaired users and also explored 13 selected authentication schemes specifically designed for blind and visually impaired users, categorizing each type of scheme according to its underlying user interaction method. Our analysis reveals that many studied schemes may not only be insecure but also often fail to meet the specific needs of blind and visually impaired users, even when specifically designed for them. We found that most schemes struggle to balance accessibility and security, with many security issues arising from accessibility challenges, particularly in screen reader-assisted interaction scenarios. Our research urges researchers, developers, and policymakers to address these gaps and develop secure, accessible solutions for blind users.

1 Introduction

Authentication schemes are crucial for securing user data and sensitive information from unauthorized access. Various security risks, including physical observation [26, 27], malware [40], phishing [132], guessing [64], concurrency [71, 82, 100], fatigue [65], downgrading [124], and cross-service [82] attacks, have been introduced to compromise the security of authentication systems. To counter these attacks, researchers continually develop various authentication schemes [1, 22, 61, 79, 129]. However, most research and development in this area focuses on the general user, neglecting the needs of special groups such as blind and visually impaired

users. This oversight is significant because about 2.2 billion people worldwide experience vision problems, with around 1.2 billion cases potentially incurable [133]. Using assistive technologies [39, 53, 86, 99, 109, 115], many individuals from this community regularly engage with smartphones, computers, and the internet to manage their online banking, personal accounts (such as email), and access a range of web services, including social media. Moreover, large-scale data breaches could occur in an organization if a blind or visually impaired employee's account is compromised, allowing unauthorized access to sensitive organizational data [7].

The primary aim of this research is to evaluate the security and accessibility of academic authentication schemes from the perspective of blind and visually impaired users and seek to identify the barriers, risks, and the need for awareness among researchers when developing authentication schemes. Because blind and visually impaired users face accessibility issues in selecting a strong password [48, 103], moreover, they face challenges in typing passwords on smartphones [8, 74], express security concerns when inputting passwords [55], and face authentication interface issues [135].

Recent research has explored security concerns for blind and visually impaired users, including visual and aural eavesdropping, transaction, and social media hacks [2, 102]. Studies have highlighted challenges such as unauthorized software installations [107] and login session timeouts [135]. Additionally, research has improved email security with phishing indicators for blind and visually impaired individuals [134]. Screen reader accessibility and security analysis have revealed navigation difficulties, risks with headphone usage, and hinders users' ability to detect risks [2, 95]. Researchers have identified accessibility and security challenges in web authentication, particularly in locating and verifying authentication pages [42], as well as vulnerability to eavesdropping [62, 116].

However, existing research has not thoroughly investigated the evaluation of widely proposed academic authentication methods regarding both security and accessibility from the perspective of blind and visually impaired users. This lack of investigation extends to understanding how these methods

interact with screen readers and how these screen readers respond to various security risks inherent in different academic authentication schemes. Expanding research in this direction could offer valuable insights into enhancing awareness among authors to ensure the security and accessibility of authentication processes for visually impaired individuals in future developments. In this paper, we aim to address this gap by examining academic authentication schemes to uncover their accessibility and security challenges. As a primary assistive technology, screen readers are crucial for blind and visually impaired users to access digital services [15, 41, 131]. In our evaluation, we analyzed security risks based on the assumption that screen readers were used, even if the authentication scheme did not explicitly state compatibility with them.

To conduct our analysis, we established criteria for selecting authentication schemes, categorized them into general schemes and those tailored for blind and visually impaired users, and used *Authentication Literature Evaluation for Security and Accessibility (ALESA)* framework designed for diverse groups to assess their security and accessibility.

Our Contributions: Main contributions are outlined below:

1. ***An accessibility and security assessment framework for diverse user groups, specifically the blind and visually impaired.*** We designed ALESA framework inspired by Bonneau et al. [25], which we updated and expanded to address the specific accessibility and security challenges faced by diverse user groups, in particular, blind and visually impaired users. We aimed to generalize the framework to accommodate other user groups who rely on screen reader assistance, such as those with dyslexia, learning disabilities, older adults facing difficulties with small text on screens, and individuals with motor disabilities. Security risks in the framework have been explained with scenarios from the perspective of target users. However, this research specifically focuses on blind and visually impaired users.
2. ***Categorization of relevant academic authentication schemes subjected to our study.*** We selected 50 papers (24.63% of 203 reviewed) based on a rigorous screening criteria that included independent review of titles, abstracts, full texts, methodological rigor (e.g., implemented and evaluated), citation count, and venue reputation. These papers were categorized into general schemes and those dedicated to blind and visually impaired users. Each academic authentication scheme was further classified based on its medium of interaction, such as login terminal interaction (e.g., OTP), user-assisted (e.g., push notification), and automatic (e.g., audio signal) verification.
3. ***Systematic evaluation of accessibility and security against the framework applying the codebook.*** Applying the codebook, which defines specific criteria for each ALESA metric, we conducted a detailed analysis of various authentication schemes for accessibility issues, specifically focusing on factors relevant to blind and visually impaired users. We systematically evaluated the work-

flows, methodologies, and full texts of these schemes and conducted a manual coding using the codebook to assess security risks from the perspective of our target users, examining potential vulnerabilities to various attacks. Our findings reveal significant accessibility and security vulnerabilities in the selected authentication schemes. None of the general authentication schemes considered accessibility during their development, resulting in incompatibility with screen readers and inaccessible interfaces. This oversight extended even to authentication schemes designed for blind and visually impaired users. On the security front, we identified risks associated with both general and schemes specifically dedicated to blind and visually impaired users. While many schemes designed for blind and visually impaired users claim resilience against certain security threats, our analysis found that they perhaps remain vulnerable to various security risks. Also, these schemes face challenges in balancing accessibility and security.

2 Background

2.1 General Principles of Authentication

Various authentication systems secure online platforms using one or more factors: something the user knows (e.g., user ID and password [13, 85]), something the user has (e.g., a smart card or smartphone generating a one-time password [73]), and something the user is (e.g., biometric characteristics like fingerprints or facial recognition [45, 49]). Authentication types are divided into three categories: single-factor authentication (SFA), requiring something the user knows [13, 85]; two-factor authentication (2FA), combining something the user knows with something they have or are [50]; and multi-factor authentication (MFA), which uses two or more factors, such as a password, an OTP, and biometric data [21, 88].

2.2 Scope of Existing Frameworks

Bonneau et al.'s [25] framework evaluates the usability of authentication schemes based on several criteria. These criteria are designed to ensure that authentication schemes are easy to use and reliable for the general user population. While this framework is comprehensive in its assessment of general usability, there are additional aspects related to the unique accessibility needs of diverse groups, such as blind and visually impaired users, that can be considered.

For instance, the framework does not explicitly address screen reader compatibility, which benefits not only users with visual impairments but also individuals with learning disabilities [34], cognitive disabilities [105], physical disabilities [94], and older users [31]. Additionally, evaluating the simplicity of performing authentication tasks and the design of accessible interfaces, including layout, application structure, and screen reader compatibility, can further enhance the

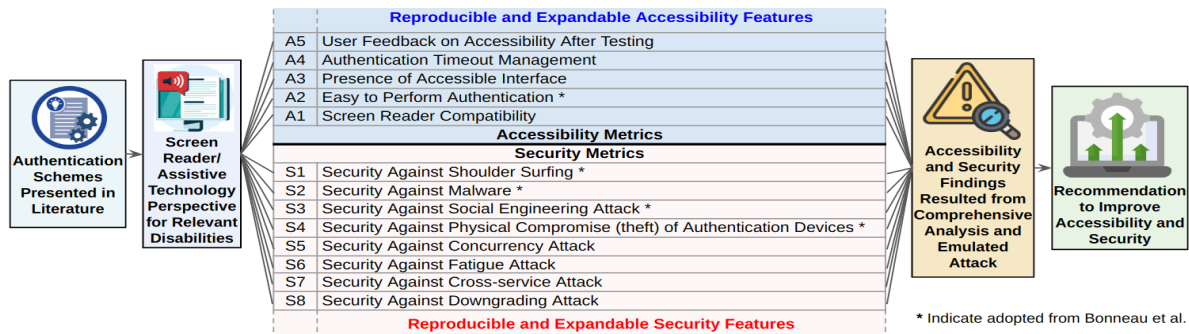


Figure 1: Overview of our ALESA framework.

user experience for various groups. Managing authentication timeouts is another important aspect for users who may require more time to complete authentication steps.

Furthermore, defining security features to specifically cover diverse groups, such as blind and visually impaired users, can enhance the overall evaluation of authentication schemes. For example, a general user can detect a malicious link by carefully observing it [35]. However, blind and visually impaired users rely on screen readers to obtain link information, which may not accurately convey the nuances of malicious links, making it harder for these users to identify potential threats.

By addressing these aspects, our research builds on Bonneau et al.'s framework by defining, enhancing, and expanding essential accessibility and security metrics, creating a more inclusive evaluation of authentication schemes.

3 Our ALESA Framework

This section outlines the development and application of our framework to evaluate academic authentication schemes for screen reader-assisted blind and visually impaired users, focusing on accessibility and security, while also explaining the replicability and broader applicability of ALESA to other relevant user groups and assistive technologies. *As a low-cost, scalable analytical tool, our framework identifies critical issues early in the design process, serving as a precursor to more extensive evaluation methods like user studies.*

3.1 Development of ALESA

Adapting Bonneau et al.'s model [25], we started with their proposed usability and security features and analyzed them from the perspective of blind and visually impaired users. This involved conducting an in-depth review of the existing literature to understand how specific risks (e.g. phishing) pose unique challenges for these users. We also examined real-world scenarios—such as how screen reader-assisted authentication behaves during phishing attacks—to assess how such risks manifest in practice. Based on these findings, we refined our selection of relevant metrics. Furthermore, we

extended the framework by incorporating additional metrics informed by both prior research and the specific needs of blind and visually impaired users. For instance, having an *accessible interface* with well-structured content is essential for blind and visually impaired users to access websites effectively—as emphasized in the W3C accessibility guidelines [127]—warranting its use as an accessibility metric, (see Fig. 1).

While several authentication schemes [81, 123], attack frameworks [6], and SoK studies [24, 84] have expanded on Bonneau's framework, but they do not explicitly consider the needs of diverse user groups (e.g., blind users). Although prior adaptations—such as Stephenson et al.'s SoK [117] on AR/VR—evaluate accessibility, they do so based on limited feedback (only 4 participants mentioned accessible). In contrast, ALESA provides a broader, interface-level analysis of accessibility and accessibility-triggered security issues, grounded in real-world screen reader interaction.

3.1.1 Accessibility Metrics

Accessibility refers to the features of an environment (e.g., physical, digital, and conceptual) that enable individuals with disabilities (vision, hearing, cognitive, motor) to enter, navigate, comprehend, and effectively use the features of that environment [56]. In our research, to assess the accessibility of selected academic authentication schemes for blind and visually impaired users, we compiled information related to various metrics relevant to accessibility for these users in our framework. These metrics are listed and explained below:

A1. Screen Reader Compatibility. Screen reader technology is one of the core mediums of interaction with digital services such as the internet, smartphones, and computers for blind and visually impaired users [41]. Therefore, the compatibility of authentication schemes with screen readers is vital, as it enables these users to perform authentication effectively. To ensure compatibility and allow screen readers to communicate the authentication scheme's functionality via audio instructions, authentication schemes need to be developed by following accessibility standard guidelines, such as with proper content structure and including alternative text for visual media (e.g., images and buttons) [126]. Recogniz-

ing the importance of screen reader compatibility based on the above analysis, we included it as an accessibility metric in our framework and aimed to evaluate whether academic authentication schemes are compatible with screen readers.

A2. Easy to Perform Authentication. Easiness refers to the characteristics of a product or service that simplify its operation and is a key aspect of accessibility [118]. It positively impacts the user experience of blind and visually impaired individuals [69]. Studies also show that these users often consider an authentication method to be accessible when it is easy to use [30]. Hence, as part of the framework, we selected easy to perform authentication as an accessibility metric to evaluate the simplicity of the authentication process. This involves minimizing the need for users to perform multiple operations or transitions between applications, such as shifting between the login window and the authenticator app.

A3. Presence of Accessible Interface. Shera et al. [112] analyzed literature and conducted tests on mobile applications to identify common interface accessibility issues faced by blind and visually impaired users. These issues include presentation problems (e.g., layout, style, text), organizational challenges (e.g., application structure, page content serialization, information overload), and behavioral issues (e.g., screen reader conflicts, redundant information). The need to address such interface-related accessibility issues is also emphasized in the W3C accessibility guidelines [127]. Hence, as part of the framework, we considered the accessibility of the authentication interface to determine if developers considered presentation problems, organizational challenges, and behavioral issues for blind and visually impaired users during the design and development of authentication scheme interfaces. If this feature is lacking, it indicates blind and visually impaired users would face difficulty during the authentication.

A4. Authentication Timeout Management. Blind and visually impaired users often face challenges in completing authentication, as they may need additional time to read content or perform tasks such as entering authentication codes; strict timeouts can therefore make the process frustrating and inaccessible [44, 135]. To evaluate whether academic authentication schemes accommodate these needs—such as by managing timeouts for diverse users (blind and visually impaired users) or minimizing complex steps—we included this feature as an accessibility metric in our ALESA framework.

A5. User Feedback on Accessibility After Testing. In addition, we considered users' opinions on accessibility by focusing on surveys conducted in the selected papers to gather participants' feedback on accessibility after letting them test the schemes. The surveys provide valuable insights into user experience and satisfaction levels, contributing to a comprehensive evaluation of the authentication schemes. This user-centered evaluation is essential, as many usability failures arise from mismatches between system design and human behavior [38]. In our research, we referred to general participants as non-

blind participants and specified other types of participants, such as blind or visually impaired.

3.1.2 Security Metrics

Blind and visually impaired users are perhaps more vulnerable to various security risks and attacks compared to sighted individuals due to limitations in visual perception [3, 108]. This part of the framework details the potential security risks and attack scenarios that screen reader assisted users, such as blind and visually impaired individuals, may face during authentication. These risks and attacks have been selected as security metrics in our framework, and the corresponding attack scenarios were applied to evaluate schemes.

S1. Security Against Shoulder Surfing. Shoulder surfing occurs when an attacker observes a victim's login process, such as entering credentials, without their knowledge [28]. This type of attack can be facilitated by hidden cameras or microphones. Blind and visually impaired users are particularly vulnerable to such attacks because they cannot detect attackers [57] or monitoring devices [108]. Screen readers audibly read display text [72] as part of their normal behavior, including credentials during the login process or when receiving OTPs on smartphones for authentication. This is an alarming risk for blind and visually impaired users compared to sighted users but they can mitigate this by using headphones to prevent others from hearing the screen reader when operating a single terminal, such as a PC. However, when using two devices like a PC and a smartphone for authentication, it may not be possible to use headphones on both simultaneously, while webAIM found 49.2% users use this setting [130].

Given the security risks that blind and visually impaired users face, we included shoulder surfing as a security feature in our framework, as an attacker may use pre-installed spying devices or stay nearby to collect credentials or get access. If the victim uses a computer in a workspace (e.g., office, study, library) and wears headphones to prevent the screen reader from speaking sensitive information aloud, the smartphone may remain insecure without headphones, as explained above. The victim focusing on the PC, might not hear the second factor generated by the attacker (e.g., OTP or audio signal) from the smartphone, but the attacker could utilize it, using spying devices or staying nearby. This could delay the victim's response to the attack.

S2. Security Against Malware. Authentication schemes may introduce insecurity against malware [14]. Malware can deactivate 2FA, and some authentication systems allow deactivation without 2FA verification. After deactivation, the malware sends the first factor credentials to the attacker for unauthorized access [40]. Re-compromise is also possible through malware [122]. Blind and visually impaired users may struggle to detect malware due to their reliance on keyboards [59], and studies show that attackers often succeed in compromising their systems [60, 114]. Additionally, screen readers face

difficulty in reading security warnings [111].

Our threat model exploits these insecurities of the blind and visually impaired user to include this security threat in our framework. Specifically, we considered the lack of a proper alert system in the selected schemes designed for blind and visually impaired users, as well as the absence of implemented security methods, such as real-time malware detection algorithms and secure sandbox environments, that could allow malware silently running in the background to capture credentials during the victim's login process. In the attack scenario, the malware could block the victim's login attempt and initiate the attacker's attempt, triggering the second factor (e.g., OTP) to be sent to the victim. It may then capture and forward the second factor (e.g., OTP) to the attacker for authentication.

S3. Security Against Social Engineering Attack. Social engineering attacks involve fraudulent requests designed to trick individuals into disclosing their credentials, ultimately leading to unauthorized access to sensitive information [96]. For blind and visually impaired users, detecting such attacks may be difficult because attackers may carefully design fraudulent links and other elements on the websites that are audibly similar to the legitimate content [108]. Hence, we included this as a metric in the ALESA framework. This type of attack involves real-time phishing attacks, wherein the attackers establish one connection to the victim, pretending to be the verifier, while simultaneously maintaining another connection to the server, pretending to be the prover [25].

In our attack scenario, the attacker exploits the screen reader's inability to properly differentiate between slightly altered links. For example, a typical user can detect a malicious link by carefully observing it. However, blind and visually impaired users rely on screen readers to obtain link information, which may not accurately convey the nuances of malicious links, making it harder for these users to identify potential threats. Like other users, they do not know whether they are under attack or not. If a blind user becomes suspicious, they can read the link character-by-character, but the choice to do so requires additional keystrokes and is time-consuming. Additionally, the attackers can make malicious links very long to make such reading more difficult. Believing the link to be legitimate, the victim shares credentials such as their username, password, and OTP to allow attackers to gain access. Having strong authentication factors (e.g., biometric, passwordless) and mechanisms (e.g., double-sided verification) in the authentication scheme, a scheme could be robust against the above insecurities and may mark secure.

S4. Security Against Physical Compromise (theft) of Authentication Devices. This occurs when an attacker gains access to the object (e.g., smartphone, FIDO key) used in the scheme for authentication. Exploiting the limitations of blind and visually impaired users in assessing unsafe surroundings [4] and detecting stealing activities [3], the attacker may attempt to acquire and utilize this object to bypass authentication.

Our threat model for this attack involves a scenario where

an attacker compromises the victim's device, such as a smartphone, without the victim's knowledge. The attacker then attempts to log in to the server, which sends an OTP, ambient audio signal, or OTP encoded in an audio signal to the compromised device. For OTP-based authentication, the attacker can easily use the code to gain access. However, authentication using an ambient sound signal requires the attacker to keep the compromised device close to their terminal. The attacker's browser communicates with the victim's device to extract the OTP or compare the sound, which is then sent to the server for verification, ultimately granting authentication. Considering the above scenarios of weaknesses, we included this as a metric in our framework. Authentication schemes incorporating biometric factors (e.g., fingerprint, facial recognition) that ensure verification by real users for authentication could be resilient against this threat.

S5. Security Against Concurrency Attack. A concurrency attack occurs when an attacker attempts to log in simultaneously with the victim. This action triggers push notifications with approval prompts for both the attacker and the victim's login approach, appearing simultaneously to the victim. This could override the victim's notification by attacker ones, leading them to misconstrue the attacker's login attempt as legitimate [71, 82, 100]. Jay Prakash et al. tested this attack on 75 pairs of sighted victims and attackers, revealing that 95% accepted the attacker's push notification without any doubt [100].

Our evaluation of this attack on real-life push-based authentication schemes from the perspective of blind and visually impaired users found that assistive technologies (e.g., screen readers) are unable to effectively communicate attacker push notification information to users. Instead, they only convey the latest notification, which could be from an attacker. Based on these findings, we added this as a security metric in ALESA. In our attack scenario, to evaluate authentication schemes for users, the attacker initiates a login attempt shortly after the victim. This timing allows the attacker's push notification to override the victim's notification, perhaps leading the victim to approve the attacker's request. Based on our evaluation, the victim will not receive any information related to the attack, making them unaware of the unauthorized access attempt.

S6. Security Against Fatigue Attack. In this attack, the attacker continuously sends push notification prompts to the user until they accept after becoming mentally exhausted. This characterizes the fatigue attack, also known as MFA spamming [65]. Our evaluation of real-life push-based authentication schemes (e.g., Google push notification-based scheme for email) from the perspective of blind and visually impaired users (using a screen reader) found that these schemes cannot detect or prevent continuous malicious push notifications from attackers. Additionally, denying a push notification forwards the user to a change password window while the user still receives notifications from the attacker. This can mislead users into thinking the prompt is part of the password change

process, causing them to approve the attack—thus, based on these insights, we added this as a framework metric.

Our attack scenario to evaluate this against push notification-based authentication starts with the attacker sending notifications at short intervals. The victim might attempt to change their password but may mistakenly accept an attacker’s notification, assuming it is legitimate. Having mechanisms that can detect and alert blind and visually impaired users about continuous/ malicious push notifications is essential for ensuring the security of these authentication schemes.

S7. Security Against Cross-service Attack. In a cross-service attack, the attacker manipulates the user’s possession factor device to trick them into authenticating for a different service than intended. For instance, when the user attempts to log into Service A, the attacker prompts an approval request for Service B. If the user unwittingly approves, the attacker gains unauthorized access to Service B, potentially compromising sensitive accounts, as described by Mahdad et al. [83].

The risk escalates when essential authentication details are not effectively communicated to blind or visually impaired users. For instance, with FIDO, which utilizes a USB dongle and fingerprint for authentication on devices such as smartphones and PCs, users may receive instructions via a security message to insert the USB dongle and press their fingerprint for authentication. In a cross-service attack, the attacker may overlay this security prompt with an image. Our observations indicate that this prevents the screen reader from reading legitimate instructions, leading the user to unknowingly authenticate to the attacker’s session. To evaluate the authentication schemes against this attack, we added this to the framework and considered the scheme’s ability (mentioned in the paper) to communicate actual service names to blind users, as well as the implementation of any robust mechanisms and secure communication protocols that can prevent this type of attack.

S8. Security Against Downgrading Attack. Downgrading attacks can compromise even strong authentication schemes, as attackers use techniques like real-time phishing to bypass robust authentication methods and downgrade them to weaker ones, gaining unauthorized access. Blind and visually impaired users often struggle to identify phishing attacks, further exacerbating the risk [108]. Additionally, assistive technologies face difficulty in effectively communicating malicious links to users, as explained in 3.1.2 (S3), thus added as metric.

In this attack scenario, the attacker stays between the victim and the server. The attacker initiates the attack by sending a phishing link to the victim, collecting their credentials, and informing the victim that the strong authentication method (e.g., FIDO) has encountered an error. The attacker then asks the victim to choose a weaker method, such as OTP. Once the victim selects the weaker method, the attacker immediately attempts to log in to the victim’s account using the collected credentials. The server requests proof of strong authentication, but the attacker opts for the weaker method. The server then sends an OTP to the victim and an OTP submission prompt to

the attacker (who appears legitimate). The victim might share the OTP with the same phishing link, allowing the attacker to authenticate. We considered vulnerabilities in authentication similar to those of phishing when evaluating this attack.

3.2 Application of ALESA on Evaluating Authentication Schemes

To apply the security and accessibility metrics of the ALESA framework to authentication schemes, we examined each scheme’s authentication workflow, methodology, and full text, and conducted a manual coding process—an approach well-suited for in-depth analysis. A structured codebook guided this process, containing four key components: (1) Code – the security and accessibility metrics defined in our framework, (2) Definition – a description of what each code measures or represents, (3) What We Looked For – specific indicators or criteria in the paper used to determine the applicability of each code, and (4) Example Indicator in Paper – representative phrases or content that signal the adherence, partial adherence (e.g., when a scheme claims to be easy but requires multiple steps including app switching), or non-adherence of a given metric, as shown in Table 1. In this research, two independent coders evaluated each paper, resolving discrepancies through discussion and consensus (see Section 5).

3.3 Replicability & Broader Applicability of ALESA

The clear development and application process of ALESA, including its accompanying codebook, enables researchers and stakeholders to accurately replicate our study. Screen readers are the primary mode of digital interaction for blind and visually impaired users [15, 41], as supported by a WebAIM study reporting that nearly 90% of its users are blind and rely on screen readers to navigate digital platforms [131]. While our study focuses on blind and visually impaired users, screen readers are also used by individuals with dyslexia [33], ADHD, and motor impairments [91]. The ALESA framework is designed to be adaptable to these user groups. For example, processing information can be particularly challenging for dyslexic users [16], so authentication methods requiring substantial cognitive effort may be infeasible—justifying the inclusion of “information-intensive authentication” as an accessibility metric for this group. Furthermore, our ALESA framework is reproducible across other assistive technologies by emphasizing interaction outputs. For instance, to adapt the framework for users who rely on voice assistants (e.g., elderly [76]), researchers may need to assess how authentication schemes interact with these assistants and analyze the resulting speech outputs. This design enables future researchers to replicate, expand, and adapt the framework as accessibility and security needs evolve.

Table 1: Codebook Used to Apply ALESA Framework Metrics on Authentication Schemes.

Code	Definition	What We Looked For	Example Indicator in Paper for Compliance/ (Partial/Non)-Compliance
Accessibility Metrics			
A1: Screen Reader Compatibility	Whether the scheme can be used effectively with screen readers.	Any mention of audio cues (partial if screen readers are directly not mentioned), alternative text, accessibility standards, or screen reader support or testing.	Compliant if scheme is compatible with screen readers / TTS rather than screen reader (partial-compliance).
A2: Easy to Perform Authentication	The simplicity of performing the authentication steps.	Steps requiring no switching between apps, fewer inputs, or no visual feedback.	Not compliant if requires user to switch from browser to Authenticator or other app
A3: Accessible Interface	Whether the UI is accessible for blind users (layout, focus order, labels).	Descriptions of UI structure, mention of following W3C accessibility guidelines or presence of accessibility issues.	Not-compliant if complex layout with unlabeled buttons or design does not specify accessibility consideration.
A4: Authentication Timeout Management	Whether the system accounts for slower input time by screen reader users or no input is required to manage timeout.	Indications of customizable or extended timeouts, retries, if the method does not require input (automatic), or manage timeout for diverse users.	Non-compliant if session expires within 30 seconds/ Compliant if authentication workflows show no required user interaction.
A5: User Feedback on Accessibility After Testing	Inclusion of participant accessibility feedback from evaluations.	Whether the paper solicits user feedback on accessibility and at least 50% users marked accessible.	Participants mentioned the schemes as inaccessible / Compliant if 51% said accessible.
Security Metrics			
S1: Security Against Shoulder Surfing	Resistance against observation-based attacks (e.g., shoulder surfing).	Steps required concurrent devices (smartphone and terminal), mention of insecurity against observation attacks, or visibility of sensitive information.	Non-compliance if OTPs are sent via ambient sound to the 2FA device/ Compliance if OTPs are securely handled within device.
S2: Security Against Malware	Whether the scheme can handle malware stealing credentials or bypassing flows.	Mentions of sandboxing, malware detection, or lack of protection.	Non-compliance if input credentials in plaintext/ Compliance if securely handled.
S3: Security Against Social Engineering	Ability to resist phishing or impersonation attacks.	Bidirectional verification, secure links, UI cues, or lack thereof.	Compliant if workflows included phishing resistance (bidirectional verification).
S4: Security Against Physical Device Compromise	Resilience to theft of the authentication device.	Use of biometrics, secure storage, or fallback weaknesses.	Not compliant if there is no mention of a verification mechanism for retrieving OTPs.
S5: Security Against Concurrency Attack	Ability to detect or mitigate concurrent login attempts.	No mention of concurrent push notification handling, multi-prompt handling, or lack of detection.	Only latest push notification is read by screen reader / Block malicious prompt.
S6: Security Against Fatigue Attack	Defense against MFA spamming.	Rate limiting, push notification filtering, alert differentiation, handle continuous malicious prompt.	Compliant if repeated prompts can be flagged as malicious.
S7: Security Against Cross-Service Attack	Preventing approval for unintended services.	Context-aware prompts, domain binding, strong association mechanisms, communicate exact service.	Not compliant if push request does not specify which service it is for.
S8: Security Against Downgrading Attack	Blocking fallback to weaker mechanisms.	Forced strong authentication, resistance to downgrade attempts, weaker recovery options.	Can fallback to SMS OTP if FIDO fails (non-compliant).

4 Studied Schemes Selection & Categorization

This section reviews various academic authentication schemes, including both general schemes and those specifically designed for blind and visually impaired users.

4.1 Selection Criteria for Schemes

We conducted a systematic web search across multiple reputable academic databases, including Google Scholar, IEEE Xplore, ACM Digital Library, Springer, and USENIX with relevant keywords. For general users, we used keywords such as "authentication method" and "two-/multi-factor authentication method". For blind and visually impaired users, we used terms like "authentication methods for blind/visually impaired users" and "two-/multi-factor authentication for blind/visually impaired users" to ensure a comprehensive collection of relevant literature. We started by analyzing general academic authentication schemes to evaluate their security and vulnerability if these schemes were to be deployed for use by blind and visually impaired users. We chose these general schemes to evaluate the researchers' awareness of the needs of diverse users and to emphasize the importance of considering these needs within the community. *This is crucial because these proposed schemes may eventually be deployed in the real world, where blind and visually impaired users will also use them.* In addition, we examined authentication schemes explic-

itly designed for blind and visually impaired users, aiming to assess their compatibility with accessibility and security from the users' perspective. *For general schemes, we considered those described without specifying any particular user group or claiming to include all users.* When selecting schemes for blind and visually impaired users, we focused on those explicitly labeled for this demographic.

The selection process was carefully conducted in two phases by researchers who independently reviewed and screened each paper for relevance. Initially, papers were filtered based on their title and abstract following the web search using the relevant keywords mentioned above, while duplicates and studies focused on authentication-related analysis (e.g., not authentication methods) were excluded, resulting in a total of 203 papers. In the next phase, we performed an in-depth screening of the abstract, methodology, authentication workflow, and full text. We specifically looked for papers' methodological strength, which required the workflow to be implemented or illustrated and tested either technically or with participants, focusing on security, usability, or both—rather than just theoretical proposals. We then considered the reputation of the venue, citation count ≥ 10 , and relevance to blind and visually impaired users (for papers specifically dedicated to this group). When making our selections, we took into account at least one of these factors, along with the paper's methodological rigor (e.g., implementation and evaluation). Based on these criteria (mentioned in the second phase), we

selected 50 papers from the original 203, representing 24.63% of the total. This selection process ensured that the chosen papers were not only methodologically sound but also highly pertinent to our research objectives, providing a solid foundation for evaluating the current state of authentication methods for blind and visually impaired users.

4.2 Selected General Authentication Schemes

This section explores the characteristics of various general authentication schemes and is organized into three categories based on their authentication processes. We provide explanations of these characteristics below and align them with their respective categories.

Login Terminal Interaction Schemes. These schemes typically require users to input a One-Time PIN (OTP) from a smartphone to a terminal. While this two-factor setup enhances security, it introduces accessibility risks—screen readers vocalize OTPs, and blind users cannot use headphones on both devices simultaneously, compromising privacy. Common techniques used in selected authentication schemes of this type include OTPs generated via hash chains [36], device identifiers like IMEI [10], or browser-stored secrets [51]. Several schemes support offline use with device-specific hashing [70] or rely on algorithms like REAL [37]. Recent work explores hybrid tokens [119], blockchain-based revocation [97], multi-modal MFA using FIDO2 and backup codes [104], and threshold-based authentication combining biometrics and device trust [75]. Authors claimed to mitigate observation risks in some designs through honeypots [98] or graphical passwords to avoid cross-device input [11].

User Assisted Verification Schemes. These schemes leverage secondary devices—like smartphones, BLE tokens, or location-aware hardware—for user-driven verification through QR scanning, image matching, location confirmation, or cross-device content inspection. While reducing terminal input, they often require visual or physical comparison across devices, posing accessibility challenges. Designs of selected schemes in this category include credential relay via personal devices (e.g., DAMFA [93], MP-Auth [87], oPass [120]), location-based prompts [5], QR/image verification [43, 78, 101], browser-assisted links [63], audio-based methods [46], EEG biometrics [23, 52], and multi-modal techniques using fingerprints, facial recognition, or voiceprints [47, 106]. Some, like TwoChain [97], incorporate blockchain for decentralized key management and revocation.

Automated Verification Schemes. These schemes enable proximity-based authentication by automatically exchanging or comparing signals—such as inaudible audio, ambient sound, Bluetooth, Wi-Fi, or channel state information (CSI)—between the 2FA device and terminal, without user input. Approaches include audio-based methods like Sound-proof [67], Proximity-proof [54], SoundAuth [128], and QuickAuth [137], as well as Bluetooth or audio-based co-

location detection (e.g., Watermelon 2FA [90], 2FA-PP [125]). Advanced designs leverage Wi-Fi CSI [110], speech decoding via wearables [113], or ambient sound combined with Physical Unclonable Functions (PUFs) [136], offering seamless authentication with minimal interaction.

4.3 Selected Dedicated Schemes

In this section, we dig into a detailed exploration of the characteristics of selected authentication schemes specifically designed for blind and visually impaired users. These schemes are classified into five distinct groups based on their mode of authentication interaction. Here, we provide explanations of the characteristics derived from the proposed schemes.

Scheme Involving Typing on Terminal. This category includes a scheme that requires manual input on terminals, including QR code generation and decryption with RSA combined with a local text-to-speech (TTS) agent to convert OTP into audio [77], enabling blind users to input spoken digits.

Gesture Based Verification Schemes. These schemes rely on touch or gesture-based interactions—such as tapping, swiping, or drawing patterns—on mobile or touchscreen devices, offering alternatives to traditional text input. Some schemes map taps to alphanumeric characters and incorporate OTP-based security [20], or use image selection and grid tapping with MD5 hashing [58]. Others replace numeric input with gesture-based PIN entry [19], or decouple confirmation from entry to enhance security [32]. Techniques like swipe gestures inspired by Braille [18], gesture-based Braille input [9], and curve-based signature authentication on touchscreens [121] provide non-visual input options. VIBI [17] adds support for multiple pattern-based inputs, further improving accessibility.

Vibration Based Verification Schemes. These schemes use haptic feedback—specifically vibration patterns—for non-visual authentication on mobile devices. The approaches of selected schemes include Braille-inspired vibration patterns for passwords [12] and vibration-count-based PIN entry via button presses [66], enabling blind users to authenticate through tactile cues.

Behavior Based Verification Scheme. This category includes schemes that rely on user behavior, such as gait patterns. In our analysis, we identified one representative scheme by Haque et al. [55], which use smartphone sensors (accelerometer, gyroscope, microphone) to capture gait and voice data and authenticate users based on unique walking patterns.

Special Hardware Authentication Scheme. Schemes that use specialized devices and require specific physical actions (e.g., bending the device [29]), enabling blind users to authenticate through physical interaction, are included in this category.

5 Evaluation and Findings

This section presents the findings of our analytical evaluation aimed at systematizing knowledge of various academic

authentication schemes from the perspective of blind and visually impaired users based on the ALESA framework presented in Section 3. The evaluations are divided into two sections: general authentication schemes and those specifically dedicated to blind and visually impaired users.

5.1 Findings on General Schemes

5.1.1 Accessibility Findings on General Schemes

Table 2: Accessibility evaluation of general authentication schemes with respect to metrics from ALESA: Screen Reader Compatibility (A1), Easy to Perform Authentication (A2), Accessible Interface (A3), Manage Authentication Timeout (A4), and User Feedback on Accessibility After Testing (A5).

Category	Author/Scheme's Name	A1	A2	A3	A4	A5
Login Terminal Interaction Schemes	Chenchev [36]	○	○	○	○	○
	Kaur [68]	○	○	○	○	○
	Aloul et al. [10]	○	○	○	○	○
	WebOTP [51]	○	●	○	○	○
	Khan et al. [70]	○	○	○	○	○
	Cheng [37]	○	○	○	○	○
	Trust OTP [119]	○	○	○	○	○
	TwoChain [97]	○	○	○	○	○
	Mello et al. [104]	○	○	○	○	○
	Papaspirou et al. [98]	○	●	○	○	○
Li et al. [75]	○	○	○	○	○	
ALSaleem and Alshoshan [11]	○	●	○	○	○	
User Assisted Verification Schemes	DAMFA [93]	○	○	○	○	○
	Meher and Amin [89]	○	○	○	○	○
	Alabdulatif [5]	○	○	○	○	○
	Audiouth [46]	○	○	○	○	○
	Bialas et al. [23]	○	○	○	○	○
	Minakova and Mansurov [92]	○	○	○	○	○
	MP-Auth [87]	○	○	○	○	○
	oPass [120]	○	●	○	○	○
	2FIM [78]	○	●	○	○	○
	ImageOTP [43]	○	●	○	○	○
	2FMA-Netbank [101]	○	○	○	○	○
	SV-2FA [47]	○	○	○	○	○
	Device-aware 2FA [63]	○	○	○	○	○
	Blink to Get In [52]	○	●	○	○	○
Sajjad et al. [106]	○	○	○	○	○	
Automated Verification Schemes	Proximity-proof [54]	○	●	○	●	●
	Sound-proof [67]	○	●	○	●	●
	2FA-PP [125]	○	●	○	●	○
	Watermelon 2FA [90]	○	●	○	●	○
	SoundAuth [128]	○	●	○	●	○
	Luo et al [80]	○	●	○	●	○
	Wi-auth [110]	○	●	○	●	○
	Listening Watch [113]	○	●	○	●	○
	T2FA [136]	○	●	○	●	○
QuickAuth [137]	○	●	○	●	○	

● : Compliance ● : Partial-Compliance ○ : Non-Compliance

Accessibility Analysis of Login Terminal Interaction Schemes. As shown in Table 2, login terminal interaction schemes exhibit several accessibility issues when evaluated

using the codebook outlined in Table 1. All schemes failed to meet even the most basic metrics, including screen reader compatibility (A1), accessible interface design (A3), and timeout handling (A4). In fact, none of the schemes fully satisfied any accessibility metric, and only 3 out of 12 schemes partially met a single metric—easy to perform authentication (A2). This highlights that, even though designed for a broader user base, most of these authentication schemes did not really consider the specific needs of blind or visually impaired users.

A common issue is that many schemes require users to act quickly—such as reading an OTP from a smartphone and typing it into a terminal (Chenchev [36], Kaur [68], WebOTP [51])—which can take longer for blind users and increase the risk of timeout. Without a well-structured, accessible interface, this process becomes even more difficult. Some schemes also require switching between multiple devices or entering multiple pieces of information (e.g., entering secret key following OTP) (Aloul et al. [10], Li et al. [75], TwoChain [97], Mello et al. [104]), which adds to the complexity and introduces further accessibility barriers. Even though a few schemes in this category claim to be “easy to use”, they still involve steps like checking the browser or verifying OTPs (ALSaleem and Alshoshan [11], WebOTP [51], Papaspirou et al. [98]), which are not fully accessible without proper implementation of accessible interfaces (e.g., guiding blind users through the authentication process)—hence, they were marked as partially meeting the metric. None of the evaluated schemes reported testing with participants for accessibility feedback (A5), highlighting a gap in inclusiveness.

Accessibility Analysis of User Assisted Verification Schemes.

User assisted verification schemes exhibit notable accessibility shortcomings under the ALESA framework and face similar challenges to those seen in login terminal interaction schemes. None of the evaluated schemes fully satisfied more than one accessibility metric, and most failed to support critical aspects such as screen reader compatibility (A1), accessible interface design (A3), and timeout management (A4). Only 4 out of 15 schemes successfully met the A2 metric (easy to perform authentication), typically minimizing the number of steps required during the verification process.

One recurring barrier is the expectation that users will interact visually with a smartphone (e.g., confirming a push notification, verifying a location) without considering how these tasks are handled by diverse users, such as blind users using screen readers (Alabdulatif [5], Audiouth [46], Meher and Amin [89], DAMFA [93]). These actions demand precise touch navigation and visual awareness, posing difficulty for blind users in the absence of proper assistive features. Schemes relying on biometric and neural signals, like facial recognition based input, introduce additional accessibility concerns due to the need for visual calibration or feedback interpretation (Bialas et al. [23], Minakova and Mansurov [92], Sajjad et al. [106]). These systems often lack audio or tactile cues, making them unsuitable for screen reader users.

Authentication flows that depend on visual comparison or interactive web components, such as QR code scanning or clickable verification links, also show poor accessibility adaptation (SV-2FA [47], Device-aware 2FA [63], MP-Auth [87], 2FMA-Netbank [101]). Without structured navigation and labeled elements, blind users face substantial difficulty completing these processes. Some user assisted schemes perform better in terms of ease of use (A2), particularly when they avoid complex multi-step operations or app switching. These schemes typically require minimal user input—such as entering a user ID or using EEG signals from eye blinks for authentication, relying on natural, involuntary actions rather than visual inputs—which reduces cognitive and physical effort for blind users (ImageOTP [43], Blink to Get In [52], 2FIM [78], oPass [120]). However, despite this improvement, none of these schemes meet any other accessibility metrics of ALESA, which highlights significant gaps in addressing real-world accessibility needs. Moreover, this ease of use (A2) adherence alone may not sufficiently support blind users, even though these schemes are intended for all users.

Accessibility Analysis of Automatic Verification Schemes.

Automatic verification schemes demonstrate relatively better accessibility characteristics under the ALESA framework compared to other general-purpose authentication categories. These schemes often meet key accessibility metrics such as ease of use (A2) and timeout resilience (A4), primarily due to their automated nature, which eliminates the need for direct user interaction during the authentication process (Sound-proof [67], Proximity-proof [54], Watermelon 2FA [90], SoundAuth [128], Luo et al. [80]). This automation helps reduce the cognitive burden associated with visually navigating authentication prompts. Even in cases where minimal interaction is required—such as device proximity or passive audio feedback—the schemes reduce reliance on vision and manual input, lowering the accessibility barrier for blind and visually impaired users (2FA-PP [125], Wi-auth [110], Listening Watch [113], QuickAuth [137]). Additionally, some schemes were evaluated through user studies that included accessibility as a metric, but only 2 out of 10—Proximity-proof [54] and Sound-proof [67]—were reported as accessible (A5), although these were conducted with sighted participants.

However, despite the apparent benefits of schemes in this category, concerns remain about their real-world accessibility. An unresolved issue is whether these systems effectively communicate necessary steps to users relying on assistive technologies like screen readers (A1). For instance, schemes that transmit OTPs via ambient sound require users to place their phone near a terminal—an instruction like “please keep your phone close to the terminal” must be conveyed accessibly. Moreover, the design of the login interface is unclear, especially regarding accessibility (A3) and screen reader support (A1). While automation offers inherent accessibility advantages, its full potential remains unrealized without inclusive design and testing with assistive technology users (A5).

5.1.2 Security Findings on General Schemes

This section explores security and attack considerations for general authentication schemes from the viewpoint of blind and visually impaired users. We have analyzed the authentication schemes to assess security risks and considerations applying the codebook (Table 1) for each risk and attack outlined in ALESA (Figure 1). Our observation revealed critical vulnerabilities in these authentication schemes when assessed from the perspective of blind and visually impaired users, as shown in the Appendix Table 5.

Security Analysis of Login Terminal Interaction Schemes.

Schemes in this category—such as those by Chenchev [36], Kaur [68], Aloul et al. [10], Khan et al. [70], Cheng [37], Papaspirou et al. [98], and ALSaleem and Alshoshan [11]—share a common structure: the user retrieves an OTP on a smartphone (2FA device) and inputs it on a separate login terminal (PC). This interaction model consistently introduces accessibility problems (Section 5.1.1) and triggers vulnerabilities across multiple security dimensions. The physical separation between the login device and the 2FA device, while secure for many sighted users, exposes the OTP to shoulder surfing (S1)—especially when screen readers vocalize sensitive content (e.g., OTP) aloud and blind or visually impaired users cannot use headphones on both devices concurrently—as emphasized in Section 3.1.2. Across different metrics, we observe a lack of robust hardware-based protections or interface obfuscation techniques, making most schemes susceptible to malware interception (S2) and device theft (S4). Notably, many schemes adopt traditional OTP workflows without introducing strong assurances against credential compromise or fallback manipulation—creating cascading vulnerabilities when users unknowingly fall back to weaker mechanisms under adversarial pressure (e.g., through phishing (S3) or downgrading attacks (S8)). These structural similarities suggest that the interaction pattern itself—decoupling authentication retrieval and input—serves as a systemic weakness across otherwise diverse proposals.

Despite these systemic shortcomings, a few (3 of 12) schemes stand out for their efforts to mitigate specific security risks through thoughtful design choices. TrustOTP [119] demonstrates the most comprehensive security posture by leveraging ARM TrustZone to isolate the authentication process and restrict OTP visibility, thus protecting against both shoulder surfing (S1) and malware (S2). Its secure display, operating within ARM TrustZone hardware, further defends against phishing (S3), cross-service attacks (S7), and downgrading attacks (S8) by isolating it from potential compromises, though it lacks built-in safeguards for stolen device scenarios (S4). Li et al.’s scheme [75] similarly adopts robust protections by obfuscating inputs using encrypted and randomized mappings (S1), employing secure local storage (S4), and integrating session management (S7). However, it overlooks phishing and downgrade attack vectors (S3, S8), which

are often linked. TwoChain [97] also strengthens resistance to shoulder surfing and malware (S1, S2) by performing local cryptographic signing of OTPs using private keys, ensuring no sensitive data is exposed during transmission or display. Still, it fails to address phishing (S3), device theft (S4), and fallback abuse (S8). These comparatively secure schemes highlight a key design insight: integrating secure isolated or cryptographic operations locally on the user’s device significantly improves resistance across multiple threat models. However, such approaches remain the exception, not the norm of general authentication schemes, underscoring the need for future schemes in this category to adopt holistic threat modeling for diverse users rather than narrowly focusing on certain groups.

It is important to mention that most of the schemes—except Mello et al. [104]—from this category are not a target of concurrency (S5) and fatigue (S6) and hence considered secured against these attacks, as in our evaluation they are considered push-notification-based risks. Furthermore, despite offering strong authentication methods (e.g., FIDO2, phone prompts), Mello et al. [104] are vulnerable when authenticating via backup codes (S1) and are hence marked as partially met.

Security Analysis of User Assisted Verification Schemes. The schemes in this category commonly rely on biometric input, device-based validation, and user confirmation through push notifications, facial recognition, or EEG signals. These interaction models limit visible credential exposure and reduce reliance on terminal-based entry, thereby avoiding many vulnerabilities seen in login-terminal OTP workflows. While this mitigates risks like shoulder surfing (S1), the dependence on a trusted device introduces risks if that device is compromised (S4). Most schemes do not offer robust mechanisms for revalidating user identity or revoking credentials when a device is lost or stolen. Moreover, schemes relying on biometric still images or audio inputs—such as Minakova and Mansurov’s [92]—may be tricked via social engineering (S3) if blind users are deceived into granting access with slightly altered malicious links. Similarly, 2FMA-NetBank [101] permits OTP-based input, making it vulnerable to shoulder surfing (S1), malware interception (S2), and phishing attempts (S3). MP-Auth [87] and oPass [120] are also exposed to malware risks (S2), as malware could forward captured login data or OTPs to attackers. Furthermore, schemes like DAMFA [93] and Minakova and Mansurov [92] do not enforce strict service-level credential isolation, leaving them open to cross-service exploitation (S7) if identifiers are reused across platforms.

Among the schemes evaluated, several stand out for implementing strong protections across a wide threat spectrum. DAMFA [93] and Białas et al. [23] combines decentralized authentication, cryptographic safeguards, and user-specific biometric signals to defend against malware (S2), theft (S4), and downgrading attacks (S8). Alabdulatif et al. [5] and Meher and Amin [89] further demonstrate how contextual cues such as proximity, registered device checks, and location verification enhance security, particularly against concurrency (S5)

and fatigue-based (S6) attacks. Although most schemes in this category avoid concurrency and fatigue risks due to their non-repetitive, biometric, or contextual workflows (e.g., not a push based authentication), there are exceptions. For instance, ImageOTP [43] requires visual comparison across devices, increasing cognitive load and susceptibility to fatigue-related errors (S6) (e.g., a victim might become mentally fatigued and randomly click an image, potentially matching the attacker’s image and allowing unauthorized access). MP-Auth [87] also remains vulnerable to concurrency attacks (S5), where users could unknowingly authorize malicious logins during simultaneous login attempts. These outliers emphasize that even in interaction models designed for usability, attention must be paid to fallback paths and user decision flow. Finally, these examples indicate that while user-assisted verification avoids many input-based threats, its security depends heavily on device trust, biometric robustness, inter-service isolation, and the inaccessibility faced by blind and visually impaired users (e.g., a screen reader’s inability to distinguish slightly altered malicious links from legitimate ones).

Security Analysis of Automatic Verification Schemes. Schemes in this category typically automate the authentication process using Bluetooth, ambient sound, or proximity-based signals, requiring the 2FA device to be physically near the login browser. This automation simplifies user interaction and eliminates the need to manually input credentials, but it introduces distinct security challenges. Because authentication is triggered passively, these schemes are exposed to shoulder surfing risks (S1), particularly in public settings where an attacker in close proximity could exploit ambient signals to hijack a session (Section 3.1.2). The reliance on proximity also makes them susceptible to physical compromise (S4); if the user’s 2FA device is stolen, an attacker can authenticate simply by placing it near a login terminal. Cross-service attacks (S7) pose another concern, especially when users cannot distinguish between legitimate and spoofed login approaches—an issue exacerbated for blind users if clear instructions are not conveyed via accessible modalities (e.g., screen readers). Despite these vulnerabilities, the risk of malware (S2), phishing (S3), concurrency (S5), and fatigue-based attacks (S6) remains minimal in this category, as these schemes do not rely on user input, push notifications, or interactive prompts. Their security model relies on spatial proximity, reducing traditional attack exposure but requiring stronger protection against physical and environmental threats.

5.1.3 Insights and Lesson Learned on General Schemes

Our cross-category analysis of general authentication schemes reveals systemic shortcomings in both accessibility and security for blind and visually impaired users. Login terminal interaction schemes consistently fail to meet even basic accessibility metrics such as screen reader compatibility (A1), accessible interface design (A3), and timeout handling

(A4), while also exhibiting widespread security vulnerabilities—particularly to shoulder surfing (S1), malware (S2), and fallback abuse (S8)—due to the reliance on terminal input and decoupled 2FA flows. User assisted verification schemes show marginal improvements in ease of use (A2) but still lack interface accessibility (A3) and are often insecure if the device is lost (S4) or if identifiers are reused across services (S7). Notably, only a few schemes such as DAMFA [93] and Bilas et al. [23] incorporate multi-layered protections spanning both accessibility and security dimensions. Automatic verification schemes offer better accessibility due to low interaction needs, supporting A2 and A4. However, their passive design introduces vulnerabilities to proximity-based threats (S1, S4) and cross-service confusion (S7), especially without screen reader-accessible feedback. Another concern is that only 6 of 37 schemes were tested with general participants and only 2 were marked as accessible by them. Together, our findings underscore that none of the categories adequately address both accessibility and security in a balanced and inclusive manner, indicating a critical need for unified, accessibility-aware threat modeling in future authentication designs.

5.2 Findings on Dedicated Schemes

5.2.1 Accessibility Findings on Dedicated Schemes

Accessibility Analysis of a Scheme involving Typing on Terminal. Table 3 shows that the scheme involving terminal typing presents serious accessibility challenges for blind users, even though it was specifically designed for them, as evaluated using the codebook (Table 1). Longhua’s scheme [77] uses a TTS agent to deliver decrypted OTPs but still relies on QR codes and multi-step visual workflows requiring manual input. While it provides speech-based instructions, the lack of explicit screen reader support creates uncertainty (A1), so it is marked as partially met. The absence of an accessible interface (A3), timeout handling (A4), and user testing (A5) further limits its overall accessibility (A2).

Accessibility Analysis of Gesture Based Verification Schemes. Gesture-based authentication schemes developed for blind and visually impaired users often aim to minimize visual input by relying on taps, swipes, or haptic feedback. As shown in Table 3, all of these schemes are easy to perform (A2), but 3 of 8 show limitations in supporting screen reader compatibility (A1) and accessible interfaces (A3). However, the major concerns lie in managing authentication timeouts (A4) and testing the schemes with real users (A5). While BlindLogin [58], ARJUNA [18], and VIBI [17] provide accessible interfaces and support screen readers (A1, A3), only VIBI includes timeout management (A4). Schemes like Banerjee and Hasan’s [20], TouchIn [121], and Balayogi and Kuppusamy [19] require minimal visual interaction but lack screen reader integration (A1) and timeout handling (A4), limiting their overall accessibility. Although many of these schemes

reduce visual dependence through gesture-based input, the absence of usability testing and incomplete implementation of accessibility features (e.g., structured guidance and timeout safeguards) highlights persistent barriers for blind users.

Table 3: Accessibility evaluation of dedicated authentication schemes with respect to metrics from ALESA: Screen Reader Compatibility (A1), Easy to Perform Authentication (A2), Accessible Interface (A3), Manage Authentication Timeout (A4), and User Feedback on Accessibility After Testing (A5).

Category	Author/Scheme’s Name	A1	A2	A3	A4	A5
Schemes involving Typing on Terminal	Longhua [77]	●	○	○	○	○
Gesture Based Verification Schemes	Banerjee and Hasan [20]	○	●	○	○	○
	BlindLogin [58]	●	●	●	○	○
	Balayogi and Kuppusamy [19]	○	●	○	○	○
	Caporusso [32]	●	●	●	○	●
	ARJUNA [18]	●	●	●	○	○
	BraillePassword [9]	●	●	●	○	○
	TouchIn [121]	○	●	●	○	●
VIBI [17]	●	●	●	●	○	
Vibration Based Verification Schemes	Alsuhbany [12]	○	●	○	●	●
	OneButtonPIN [66]	●	●	●	●	●
Behaviour Based Scheme	Haque et al. [55]	○	●	○	●	○
Special Hardware Based Scheme	BendyPass [29]	○	○	○	○	○

● : Compliance ● : Partial-Compliance ○ : Non-Compliance

Accessibility Analysis of Vibration Based Verification Schemes. Vibration-based authentication schemes perform quite well, as they leverage tactile feedback to support blind and visually impaired users through non-visual interaction. OneButtonPIN [66] meets all accessibility metrics by enabling PIN entry through vibration counting, requiring no visual input. Alsuhbany’s scheme [12] uses distinct vibration patterns for grid navigation, enhancing touch-based interaction, though it lacks screen reader support (A1). Both were tested with blind participants (A5), confirming accessibility.

Accessibility Analysis of a Behavior Based Scheme. The behavior-based scheme by Haque et al. [55] demonstrates promising accessibility due to its passive design. By using smartphone sensors to capture gait and voice data, the scheme enables background authentication without active input, supporting ease of use (A2) and timeout management (A4). However, the lack of screen reader compatibility and accessible interface design (A1, A3) raises concerns, especially during initialization and pre/post-authentication phases for blind users.

Accessibility Analysis of a Special Hardware Based Scheme. The hardware-based scheme BendyPass [29] aims to provide tactile input for blind users but does not mention anything about its accessibility and thus does not meet any metrics of ALESA. Although ease of use (A2) was hypothesized, no practical evaluation was conducted to support this claim.

5.2.2 Security Findings on Dedicated Schemes

Security Analysis of a Scheme Involving Typing on Terminal.

Table 4 shows that, based on our attack scenarios from Section 3.1.2 and the codebook in Table 1, Longhua’s authentication scheme [77] is susceptible to shoulder surfing (S1), malware (S2), social engineering (S3), physical device compromise (S4), and cross-service attacks (S7), as the scheme involves multiple steps with manual OTP entry. Concurrency (S5) and fatigue attacks (S6) do not target this type of scheme.

Table 4: Security evaluation of dedicated authentication schemes with respect to metrics from ALESA: Security Against Shoulder Surfing (S1), Security Against Malware (S2), Security Against Social Engineering (S3), Security Against Physical Compromise (theft) (S4), Security Against Concurrency (S5), Security Against Fatigue Attack (S6), Security Against Cross-service (S7), Security Against Downgrading Attack (S8).

Category	Author/Scheme’s Name	S1	S2	S3	S4	S5	S6	S7	S8
Schemes involving Typing on Terminal	Longhua [77]	○	○	○	○	●	●	○	○
Gesture Based Verification Schemes	Banerjee and Hasan [20]	○	○	○	○	●	●	○	○
	BlindLogin [58]	○	○	○	○	●	●	●	○
	Balayogi and Kuppusamy [19]	○	○	○	○	●	●	●	○
	Caporusso [32]	●	○	●	○	●	●	●	●
	ARJUNA [18]	○	○	○	○	●	●	○	○
	BraillePassword [9]	○	○	○	○	●	●	○	○
	TouchIn [121]	●	●	●	●	●	●	○	●
VIBI [17]	●	●	●	●	●	●	○	●	
Vibration Based Verification Schemes	Alsuhibany [12]	●	○	○	○	●	●	○	○
	OneButtonPIN [66]	●	○	○	○	●	●	○	○
Behaviour Based Scheme	Haque et al. [55]	●	●	●	●	●	●	○	●
Special Hardware Based Scheme	BendyPass [29]	○	○	○	○	●	●	○	○

● : Compliance ○ : Non-Compliance

Security Analysis of Gesture Based Verification Schemes.

Since gestures can be physically observed or mimicked, schemes lacking biometric enhancements are vulnerable to shoulder surfing (S1), and phishing (S3) could be exploited to collect gesture patterns for later use by an attacker, as discussed in Section 3.1.2. However, some schemes (2 of 8), TouchIn [121] and VIBI [17], introduce additional parameters such as finger pressure, which improve resistance to imitation-based threats by making gestures harder to replicate precisely. Furthermore, 5 of 8 schemes remain exposed to cross-service risks (S7) due to the lack of session isolation. These findings suggest that gesture-based schemes, despite offering non-visual interaction benefits, must incorporate multi-factor protections and session integrity to mitigate

their inherent observability risks.

Security Analysis of Vibration Based Verification Schemes.

Schemes under this category rely on vibration-based PIN entry, which limits visual observability; hence, Alsuhibany [12] and OneButtonPIN [66] are potentially secure against shoulder surfing (S1). However, due to the absence of additional security layers, these schemes remain vulnerable to other threats, as shown in Table 4. While concurrency (S5) and fatigue attacks (S6) may not be able to compromise these schemes, both remain susceptible to cross-service risks (S7).

Security Analysis of a Behavior Based Scheme. A behavior based scheme uses biometric patterns, such as gait, for authentication (here Haque et al. [55]), which are unique to each user, difficult to replicate, and secure against most attacks. However, cross-service attacks are possible, where the victim unknowingly performs actions that authenticate the attacker’s service, mistakenly believing they are completing a legitimate authentication, as explained in Section 3.1.2 (S7).

Security Analysis of Special a Hardware Based Scheme.

Observations from our attack scenarios, as detailed in Section 3.1.2, applied across each metric from ALESA, indicate that a scheme we considered in this category (BendyPass [29]) is vulnerable to multiple attacks, as the simple bend gesture required for authentication can be easily replicated.

5.2.3 Insights and Lesson Learned on Dedicated Schemes

Gesture- and behavior-based schemes generally demonstrate better performance in both accessibility and security due to their non-visual interaction models and biometric robustness. However, a notable and concerning observation is that many of these schemes—despite being explicitly designed for blind and visually impaired users—still fail to provide proper screen reader support or satisfy other critical accessibility metrics. Only a few schemes meet accessibility requirements and include tests with blind users (10 out of 13 were tested, but only 4 met accessibility criteria). On the security side, schemes leveraging biometric traits such as gait or finger pressure offer stronger resistance to specific threats. In contrast, terminal-typing schemes perform poorly in both accessibility and security, while some schemes—like OneButtonPIN [66]—demonstrate strong accessibility but lack security protections. These findings highlight the need to integrate accessibility and security holistically—ensuring that secure schemes remain usable with assistive technologies and that accessible interfaces do not introduce new security vulnerabilities. This gap underscores an important area for researchers to address in designing inclusive and resilient authentication systems.

5.3 Broader Takeaways and Lesson Learned

Below are the key takeaways and lessons from our evaluation:

- Despite a broad user focus, general authentication schemes often overlook specific user groups, particularly blind users.

- Although automated schemes offer some accessibility (easiness and timeout management), they remain vulnerable to shoulder surfing, device theft, and concurrency attacks.
- While authors of schemes specifically designed for blind and visually impaired users often claimed resistance to shoulder surfing, our analysis revealed that most still exhibited such vulnerabilities—including shoulder surfing itself—and lacked clear mention of accessibility features like screen reader compatibility or accessible interfaces. Worryingly, even user study participants did not rate these schemes highly for accessibility.
- Dedicated schemes (e.g., gesture- and vibration-based) generally perform better in terms of accessibility but often lack security protections. In contrast, general schemes—especially those using user-assisted verification—tend to offer better security but consistently fail to meet key accessibility metrics defined in ALESA.
- Many vulnerabilities in both general and dedicated schemes arise from how users interact with authentication through screen readers (e.g., not communicating service info could lead to cross-service attack).

6 Discussion

Limitations. While our study offers valuable insights into the accessibility and security vulnerabilities associated with various academic authentication schemes, we acknowledge potential limitations in our approach. In our research, we analyzed schemes for accessibility findings and critically observed the authentication workflow for each scheme, evaluating them based on the screen readers' assisted speech-based output scenario instead of an extensive evaluation with other accessibility devices used by blind and visually impaired users, such as Braille. However, it is important to note that screen readers remove the need to use specific hardware-based interfaces like Braille for blind and visually impaired users, and we also keep the ALESA framework open for future researchers to analyze schemes with other assistive technologies. Running the evaluation on the implemented environment for the schemes is not possible as they are not available by the author.

Techniques to Improve Accessibility and Mitigate Risks. This investigation indicated numerous accessibility issues and security risks that can be mitigated via proper actions by the authentication designer and the screen reader developer. One potential practical solution is an authentication scheme that minimizes the impact of physical observation and eliminates the need to type on a terminal. While an on-screen accessible drawing interface is a possibility, it should be combined with behavioral patterns, such as drawing rhythm, which is unique to each individual, to strengthen its defense against device theft and shoulder surfing. Additionally, encrypting credentials at the time of drawing on the terminal with bidirectional validation between the 2FA device and terminal can mitigate social engineering, concurrency attacks, cross-service attacks,

and malware risks. Furthermore, integrating AI into screen readers to detect phishing attempts, identify malicious links, and analyze network traffic with the help of OS-level support to flag multiple and concurrent push prompts—can help mitigate key risks. Different stakeholders—such as designers of future authentication schemes, blind and visually impaired users, relevant organizations, and security/ accessibility researchers—can use our ALESA framework to evaluate their systems for both accessibility and security by following our methodological approach and applying the codebook from Table 1, which can help uncover broader issues early on and serve as a crucial step toward informing user studies for designers, providing key insights into security and accessibility for researchers, and raising awareness among users.

Future Work. Future research should extend the evaluation to real-life authentication schemes to validate our findings in practical contexts. This could involve collaboration with technology companies to access and test their systems comprehensively. Further studies should also explore the intersection of accessibility and security for other user groups, such as those with cognitive disabilities or motor impairments, to develop a more inclusive framework. Additionally, incorporating the development and integration of screen reader technologies in authentication schemes is crucial for enhancing accessibility for blind and visually impaired users. Longitudinal studies could assess how updates and changes to authentication schemes impact their accessibility and security over time. Finally, developing new schemes that inherently balance accessibility and security could lead to effective and inclusive solutions.

7 Conclusion

This study underscores the significant security and accessibility challenges faced by blind and visually impaired users in academic authentication schemes. Our research reveals that many popular schemes fall short of meeting the accessibility and security needs of this demographic. We developed ALESA framework to systematically evaluate these schemes, uncovering issues like poor screen reader compatibility, complex operations, and various security vulnerabilities. The findings highlight the urgent need for secure and inclusive authentication mechanisms. Future research should validate our findings in real-world contexts, collaborate with tech companies, and focus on developing balanced authentication schemes that address both accessibility and security.

Acknowledgments

We thank our shepherd and the anonymous reviewers for their insightful comments and valuable recommendations, which greatly improved our paper. This work was supported in part by NSF grants CNS-2154507, OAC-2139358, CNS-2201465, and a DOD grant FA9550-23-1-0453.

Ethical Considerations

Although our research highlights significant security and accessibility challenges, its ethical foundation lies in the intention to enhance digital inclusivity and safety. By addressing the overlooked needs of blind and visually impaired users, we aim to raise awareness and promote research toward accessible, secure authentication methods. This work advocates for inclusive technological progress that protects all users.

Open Science

In adherence to open science principles, this paper systematically evaluates academic authentication schemes for blind and visually impaired users using public domain resources. Its primary contribution is the ALESA framework, designed to assess both accessibility and security and transparently presented in the manuscript to ensure reproducibility. The study evaluates 50 academic papers selected based on methodological rigor, relevance, citation count, and publication venue. While it does not produce experimental artifacts or software, it shares key analytical artifacts, including the list of selected schemes based on the above criteria and the application of ALESA on schemes—available at: <https://doi.org/10.5281/zenodo.15612034>. ALESA can be extended to future schemes, adapted for other disabilities (e.g., dyslexia), and applied with assistive technologies like braille displays, thereby supporting open science, collaboration, and the development of inclusive, secure authentication systems.

References

- [1] Yasmeen Abdrabou, Mohamed Khamis, Rana Mohamed Eisa, Sherif Ismail, and Amr Elmougy. Just gaze and wave: Exploring the use of gaze and gestures for shoulder-surfing resilient authentication. In *Proceedings of the 11th acm symposium on eye tracking research & applications*, pages 1–10, 2019.
- [2] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia. Privacy concerns and behaviors of people with visual impairments. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2015.
- [3] Tousif Ahmed, Roberto Hoyle, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Understanding the physical safety, security, and privacy concerns of people with visual impairments. *IEEE Internet Computing*, 21(3):56–63, 2017.
- [4] Tousif Ahmed, Patrick Shaffer, Kay Connelly, David Crandall, and Apu Kapadia. Addressing physical safety, security, and privacy for people with visual impairments. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 341–354, 2016.
- [5] Abdullah Alabdulatif, Rohan Samarasinghe, and Navod Neranjan Thilakarathne. A novel robust geolocation-based multi-factor authentication method for securing atm payment transactions. *Applied Sciences*, 13(19):10743, 2023.
- [6] Furkan Alaca, AbdelRahman Abdou, and Paul C van Oorschot. Comparative analysis and framework evaluating mimicry-resistant and invisible web authentication schemes. *IEEE Transactions on Dependable and Secure Computing*, 18(2):534–549, 2019.
- [7] Hussain Aldawood, Tawfiq Alashoor, and Geoffrey Skinner. Does awareness of social engineering make employees more secure. *International Journal of Computer Applications*, 177(38):45–49, 2020.
- [8] Maraim Alnfai and Srinivas Sampalli. An evaluation of singletapbraille keyboard: a text entry method that utilizes braille patterns on touchscreen devices. In *Proceedings of the 18th international ACM SIGACCESS conference on computers and accessibility*, 2016.
- [9] Mrim Alnfai and Srinivas Sampalli. Braillepassword: accessible web authentication technique on touchscreen devices. *Journal of Ambient Intelligence and Humanized Computing*, 10:2375–2391, 2019.
- [10] Fadi Aloul, Syed Zahidi, and Wassim El-Hajj. Two factor authentication using mobile phones. In *2009 IEEE/ACS international conference on computer systems and applications*, pages 641–644. IEEE, 2009.
- [11] Bandar Omar ALSaleem and Abdullah I Alshoshan. Multi-factor authentication to systems login. In *2021 National Computing Colleges Conference (NCCC)*, pages 1–4. IEEE, 2021.
- [12] Suliman A Alsuhibany. Vibration-based pattern password approach for visually impaired people. *Computer Systems Science & Engineering*, 40(1), 2022.
- [13] J Anderson and Rayford Vaughn. Guide to understanding identification and authentication in trusted systems (light blue book). *National Computer Security Center NCSC-TG-017*, 1991.
- [14] Eduardo de O Andrade, José Viterbo, Cristina N Vasconcelos, Joris Guérin, and Flavia Cristina Bernardini. A model based on lstm neural networks to identify five different types of malware. *Procedia Computer Science*, 159:182–191, 2019.

- [15] Andrew Arch. Assistive technology survey 2021, 2021. <https://intopia.digital/articles/assistive-technology-survey-2021-preliminary-results/>.
- [16] Øistein Anmarkrud, Eva Wennås Brante, and Anette Andresen. Potential processing challenges of internet use among readers with dyslexia. In *Handbook of multiple source use*, pages 117–132. Routledge, 2018.
- [17] V Balaji, KS Kuppusamy, and Shaikh Afzal. Vibi: a braille inspired password entry model to assist person with visual impairments. In *Smart Secure Systems–IoT and Analytics Perspective: Second International Conference on Intelligent Information Technologies. ICIIT 2017, Chennai, India, December 20-22, 2017, Proceedings 2*, pages 320–327. Springer, 2018.
- [18] G Balayogi and KS Kuppusamy. Arjuna: An accessible pin entry model in smartphones for persons with low vision. *Internet Technology Letters*, 6(6):e466, 2023.
- [19] G Balayogi and KS Kuppusamy. Touch pointer movement-based pin entry in smartphones to assist persons with visual impairments. In *International Conference on Emerging Trends and Technologies on Intelligent Systems*, pages 249–260. Springer, 2023.
- [20] Amit Banerjee and Mahamudul Hasan. Tap based user authentication on smartphones for visually impaired people. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pages 1–7. IEEE, 2018.
- [21] Sreenivasa Rao Basavala, Narendra Kumar, and Alok Agarrwal. Authentication: An overview, its types and integration with web and mobile applications. In *2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing*. IEEE, 2012.
- [22] Munmun Bhattacharya, Sandip Roy, Samiran Chattopadhyay, Ashok Kumar Das, and Sajjad Shaukat Jamal. Aspa-mosn: An efficient user authentication scheme for phishing attack detection in mobile online social networks. *IEEE Systems Journal*, 17(1), 2022.
- [23] Katarzyna Białas, Michał Kedziora, Rafał Chałupnik, and Houbing Herbert Song. Multifactor authentication system using simplified eeg brain–computer interface. *IEEE Transactions on Human-Machine Systems*, 52(5):867–876, 2022.
- [24] Jenny Blessing, Daniel Hugenroth, Ross J Anderson, and Alastair R Beresford. Sok: Web authentication in the age of end-to-end encryption. *arXiv preprint arXiv:2406.18226*, 2024.
- [25] Joseph Bonneau, Cormac Herley, Paul C Van Oorschot, and Frank Stajano. The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *2012 IEEE symposium on security and privacy*, pages 553–567. IEEE, 2012.
- [26] Leon Bošnjak and Boštjan Brumen. Shoulder surfing: From an experimental study to a comparative framework. *International Journal of Human-Computer Studies*, 130:1–20, 2019.
- [27] Leon Bošnjak and Boštjan Brumen. Shoulder surfing experiments: A systematic literature review. *Computers & Security*, 99:102023, 2020.
- [28] VA Brennen. *Cryptography dictionary*, vol. 2005, 1.0., 2004.
- [29] Daniella Briotto Faustino and Audrey Girouard. Bend passwords on bendypass: a user authentication method for people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 435–437, 2018.
- [30] Daniella Briotto Faustino and Audrey Girouard. Understanding authentication method use on mobile devices by people with vision impairment. In *Proceedings of the 20th International ACM SIGACCESS Conference on Computers and Accessibility*, pages 217–228, 2018.
- [31] Marina Buzzi, Barbara Leporini, and Clara Meattini. Design guidelines for web interfaces of home automation systems accessible via screen reader. *Journal of Web Engineering*, 18(4–6):477–511, 2019.
- [32] N. Caporusso. An improved pin input method for the visually impaired. In *2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO)*, pages 476–481, 2021.
- [33] Casandra Visser, Danny Trichter, Ajay Sohal. Unlocking potential: Assistive technology for dyslexia, 2024. <https://www.accessibilitychecker.org/blog/assistive-technology-for-dyslexia/>.
- [34] Chwen Chen, Melissa Keong, Chee Teh, and Kee Chuah. Learners with dyslexia: Exploring their experiences with different online reading affordances. *Themes in Science and Technology Education*, 2015.
- [35] Juan Chen and Chuanxiong Guo. Online detection and prevention of phishing attacks. In *2006 First International Conference on Communications and Networking in China*, pages 1–7. IEEE, 2006.
- [36] Ivaylo Chenchev. Framework for multi-factor authentication with dynamically generated passwords. In *Future of Information and Communication Conference*, pages 563–576. Springer, 2023.

- [37] Fred Cheng. Security attack safe mobile and cloud-based one-time password tokens using rubbing encryption algorithm. *Mobile Networks and Applications*, 16:304–336, 2011.
- [38] Lorrie F Cranor. A framework for reasoning about the human in the loop. 2008.
- [39] m Csapo, Gyorgy Wersenyi, Hunor Nagy, and Tony Stockman. A survey of assistive technologies and applications for blind users on mobile platforms: a review and foundation for research. *Journal on Multimodal User Interfaces*, 9:275–286, 2015.
- [40] Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi. On the (in) security of mobile two-factor authentication. In *Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18*, pages 365–383. Springer, 2014.
- [41] Bryan Dosono, Jordan Hayes, and Yang Wang. {"I'm}{Stuck!}": A contextual inquiry of people with visual impairments in authentication. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pages 151–168, 2015.
- [42] Bryan Dosono, Jordan Hayes, and Yang Wang. Toward accessible authentication: Learning from people with visual impairments. *IEEE Internet Computing*, 22(2):62–70, 2018.
- [43] Chris Drake and Praveen Gauravaram. Designing a user-experience-first, privacy-respectful, high-security mutual-multifactor authentication solution. In *Security in Computing and Communications: 6th International Symposium, SSCC 2018, Bangalore, India, September 19–22, 2018, Revised Selected Papers 6*, pages 183–210. Springer, 2019.
- [44] Ahmet Erinola, Annalina Buckmann, Jennifer Friedauer, Aslı Yardım, and M Angela Sasse. “as usual, i needed assistance of a seeing person”: Experiences and challenges of people with disabilities and authentication methods. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 575–593. IEEE, 2023.
- [45] Marcos Faundez-Zanuy. Biometric security technology. *IEEE Aerospace and Electronic Systems Magazine*, 21(6):15–26, 2006.
- [46] Muhammad Ali Fauzi and Bian Yang. Audiouth: Multi-factor authentication based on audio signal. In *Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3*, pages 935–946. Springer, 2021.
- [47] Haruhiko Fujii and Yukio Tsuruoka. Sv-2fa: Two-factor user authentication with sms and voiceprint challenge response. In *8Th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, pages 283–287. IEEE, 2013.
- [48] Steven Furnell, Kirsi Helkala, and Naomi Woods. Accessible authentication: Assessing the applicability for users with disabilities. *Computers & Security*, 113:102561, 2022.
- [49] Mary Grace Galterio, Simi Angelic Shavit, and Thailer Hayajneh. A review of facial biometrics security for smart devices. *Computers*, 7(3):37, 2018.
- [50] Paul A Grassi, Michael E Garcia, and James L Fenton. Digital identity guidelines. *NIST special publication*, 800:63–3, 2017.
- [51] Zhi Guan, Hu Xiong, Suke Li, and Zhong Chen. Mobile browser as a second factor for web authentication. In *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications*, 2011.
- [52] Ekansh Gupta, Mohit Agarwal, and Raghupathy Sivakumar. Blink to get in: Biometric authentication for mobile devices using eeg signals. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2020.
- [53] Lilit Hakobyan, Jo Lumsden, Dympna O’Sullivan, and Hannah Bartlett. Mobile assistive technologies for the visually impaired. *Survey of ophthalmology*, 2013.
- [54] Dianqi Han, Yimin Chen, Tao Li, Rui Zhang, Yaochao Zhang, and Terri Hedgpath. Proximity-proof: Secure and usable mobile two-factor authentication. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 2018.
- [55] Md Munirul Haque, Shams Zawoad, and Ragib Hasan. Secure techniques and methods for authenticating visually impaired mobile phone users. In *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, pages 735–740. IEEE, 2013.
- [56] Mark Harniss. Accessibility. In Alex C. Michalos, editor, *Encyclopedia of quality of life and well-being research*. Springer Netherlands Dordrecht, 2014.
- [57] Kirsi Helkala. Disabilities and authentication methods: Usability and security. In *2012 Seventh International Conference on Availability, Reliability and Security*, pages 327–334. IEEE, 2012.
- [58] Yean Li Ho, Bachir Bendrissou, Afizan Azman, and Siong Hoe Lau. Blindlogin: a graphical authentication system with support for blind and visually impaired users on smartphones. *Am. J. Appl. Sci*, 14, 2017.

- [59] J Holman, J Lazar, and J Feng. Investigating the security-related challenges of blind users on the web. In *Designing inclusive futures*. Springer, 2008.
- [60] Fethi A Inan, Akbar S Namin, Rona L Pogrud, and Keith S Jones. Internet use and cybersecurity concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1):28–40, 2016.
- [61] David P Jablon. Extended password key exchange protocols immune to dictionary attack. In *Proceedings of IEEE 6th workshop on enabling technologies: Infrastructure for collaborative enterprises*. IEEE, 1997.
- [62] Mohit Jain, Nirmalendu Diwakar, and Manohar Swaminathan. Smartphone usage by expert blind users. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2021.
- [63] Markus Jakobsson. Social engineering resistant 2fa. *Security, Privacy and User Interaction*, 2020.
- [64] Heasuk Jo, Yunho Lee, Mijin Kim, Seungjoo Kim, and Dongho Won. Off-line password-guessing attack to yang’s and huang’s authentication schemes for session initiation protocol. In *2009 Fifth International Joint Conference on INC, IMS and IDC*. IEEE, 2009.
- [65] Joe Köller. Mfa fatigue: Everything you need to know about the new hacking strategy, 2022. <https://www.tenfold-security.com/en/mfa-fatigue/>.
- [66] Manisha Varma Kamarushi, Stacey L Watson, Gareth W Tigwell, and Roshan L Peiris. Onebuttonpin: A single button authentication method for blind or low vision users to improve accessibility and prevent eavesdropping. *Proceedings of the ACM on Human-Computer Interaction*, 6(MHCI):1–22, 2022.
- [67] Nikolaos Karapanos, Claudio Marforio, Claudio Soriente, and Srdjan Capkun. {Sound-Proof}: Usable {Two-Factor} authentication based on ambient sound. In *24th USENIX security symposium (USENIX security 15)*, pages 483–498, 2015.
- [68] Sandeep Kaur, Gaganpreet Kaur, and Mohammad Shabaz. A secure two-factor authentication framework in cloud computing. *Security and Communication Networks*, 2022:1–9, 2022.
- [69] Akif Khan and Shah Khusro. A mechanism for blind-friendly user interface adaptation of mobile apps: A case study for improving the user experience of the blind people. *Journal of Ambient Intelligence and Humanized Computing*, 13(5):2841–2871, 2022.
- [70] Burhan Ul Islam Khan, Rashidah F Olanrewaju, Farhat Anwar, and Mashkuri Yaacob. Offline otp based solution for secure internet banking access. In *2018 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, pages 167–172. IEEE, 2018.
- [71] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. Evaluating the security posture of real-world fido2 deployments. 2023.
- [72] Jonathan Lazar, Aaron Allen, Jason Kleinman, and Chris Malarkey. What frustrates screen reader users on the web: A study of 100 blind users. *International Journal of human-computer interaction*, 22(3), 2007.
- [73] Young Sil Lee, Nack Hyun Kim, Hyotaek Lim, HeungKuk Jo, and Hoon Jae Lee. Online banking authentication system using mobile-otp with qr-code. In *5th International Conference on Computer Sciences and Convergence Information Technology*. IEEE, 2010.
- [74] Barbara Leporini, Maria Claudia Buzzi, and Marina Buzzi. Interacting with mobile devices via voiceover: usability and accessibility issues. In *Proceedings of the 24th Australian computer-human interaction conference*, pages 339–348, 2012.
- [75] Wenting Li, Haibo Cheng, Ping Wang, and Kaitai Liang. Practical threshold multi-factor authentication. *IEEE transactions on information forensics and security*, 16:3573–3588, 2021.
- [76] Mingzhou Liu, Caixia Wang, and Jing Hu. Older adults’ intention to use voice assistants: Usability and emotional needs. *Heliyon*, 9(11), 2023.
- [77] Li Longhua. A novel design of otp-based authentication scheme using smart phones and 2-d barcodes for the visually impaired. In *Proceedings of the 6th International Conference on Rehabilitation Engineering & Assistive Technology*, pages 1–4, 2012.
- [78] H Karen Lu, Asad Ali, Benoit Famechon, and Najam Siddiqui. Out-of-band authentication using 2-factor image matching. In *Proceedings of the International Conference on Security and Management (SAM)*, pages 132–140. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2019.
- [79] Yanrong Lu and Dawei Zhao. Providing impersonation resistance for biometric-based authentication scheme in mobile cloud computing service. *Computer Communications*, 182:22–30, 2022.
- [80] Jia-Ning Luo, Meng-Hsuan Tsai, Nai-Wei Lo, Chih-Yang Kao, and Ming-Hour Yang. Ambient audio authentication. *Mathematical Biosciences and Engineering*, 16(6):6562–6586, 2019.

- [81] Robbie MacGregor et al. Evaluating the android security key scheme: An early usability, deployability, security evaluation with comparative analysis. *Who Are You*, pages 1–6, 2019.
- [82] Ahmed Tanvir Mahdad, Mohammed Jubur, and Nitesh Saxena. Breaking mobile notification-based authentication with concurrent attacks outside of mobile devices. In *Proceedings of the 29th Annual International Conference on Mobile Computing and Networking*, 2023.
- [83] Ahmed Tanvir Mahdad, Mohammed Jubur, and Nitesh Saxena. Breaching security keys without root: Fido2 deception attacks via overlays exploiting limited display authenticators. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, pages 1686–1700, 2024.
- [84] Ahmed Tanvir Mahdad and Nitesh Saxena. Sok: A comprehensive evaluation of 2fa-based schemes in the face of active concurrent attacks from user terminal. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023.
- [85] Udi Manber. A simple scheme to make passwords based on one-way functions much harder to crack. *Computers & Security*, 15(2):171–176, 1996.
- [86] Kanak Manjari, Madhushi Verma, and Gaurav Singal. A survey on assistive technology for visually impaired. *Internet of Things*, 11:100188, 2020.
- [87] Mohammad Mannan and Paul C Van Oorschot. Using a personal device to strengthen password authentication from an untrusted computer. In *International Conference on Financial Cryptography and Data Security*, pages 88–103. Springer, 2007.
- [88] DT Manurung. Designing of user authentication based on multi-factor authentication on wireless networks. *Jour of Adv Research in Dynamical & Control Systems*.
- [89] Bimal Kumar Meher and Ruhul Amin. A location-based multi-factor authentication scheme for mobile devices. *International Journal of Ad Hoc and Ubiquitous Computing*, 41(3):181–190, 2022.
- [90] Joshua Meier, Jesse Zhang, Richard Zou, and James Mickens. Zero-effort two-factor authentication using audio signals. In *2017 International Symposium on Cyber Security Cryptography and Machine Learning*.
- [91] Metropolitan State University of Denver. Screen readers, 2025. <https://www.msudenver.edu/teaching-learning-design/instructional-accessibility/guides-resources/screen-readers/>.
- [92] Natalya Minakova and Alexander Mansurov. Implementing open source biometric face authentication for multi-factor authentication procedures. In *International Conference on High-Performance Computing Systems and Technologies in Scientific Research, Automation of Control and Production*. Springer, 2021.
- [93] Omid Mir, Michael Roland, and René Mayrhofer. Damfa: Decentralized anonymous multi-factor authentication. In *Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure*, pages 10–19, 2020.
- [94] Holly J Moist. Technology and disability: A help or a hindrance? 2013.
- [95] Daniela Napoli, Khadija Baig, Sana Maqsood, and Sonia Chiasson. " i'm literally just hoping this will {Work:}' obstacles blocking the online security and privacy of users with visual disabilities. In *Seventeenth Symposium on Usable Privacy and Security*, 2021.
- [96] Michael Nieves, Kelley Dempsey, Victoria Yan Pilliteri, et al. An introduction to information security. *NIST special publication*, 800(12):101, 2017.
- [97] Yustus Eko Oktian, Sang-Gon Lee, and Hoon-Jae Lee. Twochain: Leveraging blockchain and smart contract for two factor authentication. In *2020 3rd International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*. IEEE, 2020.
- [98] Vassilis Papaspirou, Maria Papathanasaki, Leandros Maglaras, Ioanna Kantzavelou, Christos Douligeris, Mohamed Amine Ferrag, and Helge Janicke. A novel authentication method that combines honeytokens and google authenticator. *Information*, 14(7):386, 2023.
- [99] Madeline Phillips and Michael J Proulx. Social interaction without vision: an assessment of assistive technology for the visually impaired. *Technology & Innovation*, 20(1-2):85–93, 2018.
- [100] Jay Prakash, Clarice Chua Qing Yu, Tanvi Ravindra Thombre, Andrei Bytes, Mohammed Jubur, Nitesh Saxena, Lucienne Blessing, Jianying Zhou, and Tony QS Quek. Countering concurrent login attacks in “just tap” push-based authentication: A redesign and usability evaluations. In *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2021.
- [101] Andreyanto Pratama and Edit Prima. 2fma-netbank: A proposed two factor and mutual authentication scheme for efficient and secure internet banking. In *2016 8th International Conference on Information Technology and Electrical Engineering (ICITEE)*. IEEE, 2016.

- [102] Georg Regal, Elke Mattheiss, Marc Busch, and Manfred Tscheligi. Insights into internet privacy for visually impaired and blind people. In *Computers Helping People with Special Needs: 15th International Conference, ICCHP 2016, Linz, Austria, July 13-15, 2016*, pages 231–238. Springer, 2016.
- [103] Karen Renaud, Graham Johnson, and Jacques Ophoff. Accessible authentication: dyslexia and password strategies. *Information & Computer Security*, 2021.
- [104] Emerson Ribeiro de Mello, Michelle Silva Wangham, Samuel Bristot Loli, Carlos Eduardo da Silva, Gabriela Cavalcanti da Silva, Shirlei Aparecida de Chaves, and Bruno Bristot Loli. Multi-factor authentication for shibboleth identity providers. *Journal of Internet Services and Applications*, 11:1–21, 2020.
- [105] Cheryl A Riley. Libraries, aggregator databases, screen readers and clients with disabilities. *Library hi tech*.
- [106] Muhammad Sajjad, Salman Khan, Tanveer Hussain, Khan Muhammad, Arun Kumar Sangaiah, Aniello Castiglione, Christian Esposito, and Sung Wook Baik. Cnn-based anti-spoofing two-tier multi-factor authentication system. *Pattern Recognition Letters*, 126, 2019.
- [107] Graig Sauer, Jonathan Holman, Jonathan Lazar, Harry Hochheiser, and Jinjuan Feng. Accessible privacy and security: a universally usable human-interaction proof tool. *Universal Access in the Information Society*.
- [108] Nitesh Saxena and James H Watt. Authentication technologies for the blind or visually impaired. In *Proceedings of the USENIX Workshop on Hot Topics in Security (HotSec)*, volume 9, page 130, 2009.
- [109] Suraj Singh Senjam. Smartphones as assistive technology for visual impairment. *Eye*, 35(8), 2021.
- [110] Syed W Shah and Salil S Kanhere. Wi-auth: Wifi based second factor user authentication. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, pages 393–402, 2017.
- [111] Filipo Sharevski and Aziz N Zeidieh. “i just didn’t notice it:” experiences with misinformation warnings on social media amongst users who are low vision or blind. In *Proceedings of the 2023 New Security Paradigms Workshop*, pages 17–33, 2023.
- [112] Azeem Shera, Muhammad Waseem Iqbal, Syed Khuram Shahzad, Madeeha Gul, Natash Ali Mian, Muhammad Raza Naqvi, and Babar Ayub Khan. Blind and visually impaired user interface to solve accessibility problems. *Intelligent Automation and Soft Computing*.
- [113] Prakash Shrestha and Nitesh Saxena. Listening watch: Wearable two-factor authentication using speech signals resilient to near-far attacks. In *Proceedings of the 11th ACM conference on security & privacy in wireless and mobile networks*, pages 99–110, 2018.
- [114] Akbar Siami Namin, Rattikorn Hewett, Keith S Jones, and Rona Pogrud. Sonifying internet security threats. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*.
- [115] Yue-Ting Siu and Ike Presley. Access technology for blind and low vision accessibility. 2020.
- [116] Berglind F Smaradottir, Jarle A Håland, and Santiago G Martinez. User evaluation of the smartphone screen reader voiceover with visually disabled participants. *Mobile Information Systems*, 2018:1–9, 2018.
- [117] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlene Fernandes, Yuhang Zhao, and Rahul Chatterjee. Sok: Authentication in augmented and virtual reality. In *2022 IEEE symposium on security and privacy (SP)*.
- [118] Molly Follette Story. Maximizing usability: the principles of universal design. *Assistive technology*, 1998.
- [119] He Sun, Kun Sun, Yuewu Wang, and Jiwu Jing. Trustotp: Transforming smartphones into secure one-time password tokens. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pages 976–988, 2015.
- [120] Hung-Min Sun, Yao-Hsin Chen, and Yue-Hsun Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. *IEEE transactions on information forensics and security*, 2011.
- [121] Jingchao Sun, Rui Zhang, Jinxue Zhang, and Yanchao Zhang. Touchin: Sightless two-factor authentication on multi-touch mobile devices. In *2014 IEEE conference on communications and network security*. IEEE, 2014.
- [122] Kurt Thomas, Frank Li, Ali Zand, Jacob Barrett, Juri Ranieri, Luca Invernizzi, Yarik Markov, Oxana Comanescu, Vijay Eranti, Angelika Moscicki, et al. Data breaches, phishing, or malware? understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security*, pages 1421–1434, 2017.
- [123] Cristian M Toader and Frank Stajano. User authentication for pico: When to unlock a security token. *Master’s thesis, University of Cambridge*, 2014.
- [124] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing

eliminated with {FIDO}? social engineering downgrade attacks against {FIDO} protocols. In *30th USENIX Security Symposium*, pages 3811–3828, 2021.

- [125] Enis Ulqinaku, Daniele Lain, and Srdjan Capkun. 2fa-pp: 2nd factor phishing prevention. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 60–70, 2019.
- [126] W3C. Wcag 2 overview, 2007. <https://www.w3.org/WAI/standards-guidelines/wcag/>.
- [127] W3C. W3c accessibility guidelines (wcag) 3.0, 2024. <https://www.w3.org/TR/wcag-3.0/>.
- [128] Mingyue Wang, Wen-Tao Zhu, Shen Yan, and Qiongxiao Wang. Soundauth: Secure zero-effort two-factor authentication based on audio signals. In *2018 IEEE Conference on Communications and Network Security*.
- [129] Yongge Wang. Password protected smart card and memory stick authentication against off-line dictionary attacks. In *IFIP international information security conference*, pages 489–500. Springer, 2012.
- [130] WebAIM. Screen reader user survey number 8 results, 2019. <https://webaim.org/projects/screenreadersurvey8/>.
- [131] WebAIM. Screen reader user survey number 9 results, 2021. <https://webaim.org/projects/screenreadersurvey9/>.
- [132] D Yu Weider, Shruti Nargundkar, and Nagapriya Tiruthani. A phishing vulnerability analysis of web based systems. In *2008 IEEE Symposium on Computers and Communications*. IEEE, 2008.
- [133] World Health Organization. Blindness and vision impairment, 2023. <https://www.who.int/news-room/factsheets/detail/blindness-and-visual-impairment>.
- [134] Yaman Yu, Saidivya Ashok, Smirity Kaushi, Yang Wang, and Gang Wang. Design and evaluation of inclusive email security indicators for people with visual impairments. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 2022.
- [135] Alisa Zezulak, Faiza Tazi, and Sanchari Das. Sok: Evaluating privacy and security concerns of using web services for the disabled population. *arXiv preprint arXiv:2302.13261*, 2023.
- [136] Jiliang Zhang, Xiao Tan, Xiangqi Wang, Aibin Yan, and Zheng Qin. T2fa: Transparent two-factor authentication. *IEEE Access*, 6:32677–32686, 2018.

- [137] Xiaoyan Zhu, Suiyu Yu, and Qingqi Pei. Quick-auth: two-factor quick authentication based on ambient sound. In *2016 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2016.

Appendix Table

Table 5: Security evaluation on general authentication schemes with respect to metrics from ALESA: Security Against Shoulder Surfing (S1), Security Against Malware (S2), Security Against Social Engineering (S3), Security Against Physical Compromise (theft) (S4), Security Against Concurrency (S5), Security Against Fatigue Attack (S6), Security Against Cross-service (S7), Security Against Downgrading Attack (S8).

Category	Author/Scheme's Name	S1	S2	S3	S4	S5	S6	S7	S8
Login Terminal Interaction Schemes	Chenchev [36]	○	○	○	○	●	●	○	○
	Kaur [68]	○	○	○	○	●	●	○	○
	Aloul et al. [10]	○	○	○	○	●	●	○	○
	WebOTP [51]	○	○	●	○	●	●	○	●
	Khan et al. [70]	○	○	○	○	●	●	○	○
	Cheng [37]	○	○	○	○	●	●	○	○
	Trust OTP [119]	●	●	●	○	●	●	●	●
	TwoChain [97]	●	●	○	○	●	○	○	○
	Mello et al. [104]	○	○	○	○	○	○	○	○
	Papaspirou et al. [98]	○	○	○	○	●	●	○	○
	Li et al. [75]	●	●	○	●	●	●	●	○
ALSaleem and Alshoshan [11]	○	●	○	○	●	●	○	○	
User Assisted Verification Schemes	DAMFA [93]	●	●	●	●	●	●	○	●
	Meher and Amin [89]	●	●	●	○	●	●	●	●
	Alabdulatif et al. [5]	●	●	●	○	●	●	●	●
	Audiouth [46]	○	●	●	○	●	●	○	●
	Bialas et al. [23]	●	●	●	●	○	●	●	●
	Minakova and Mansurov [92]	●	○	○	○	○	●	○	○
	MP-Auth [87]	●	○	●	○	○	●	●	●
	oPass [120]	●	○	●	○	○	●	●	●
	2FIM [78]	●	●	●	○	○	●	●	●
	ImageOTP [43]	●	●	●	○	○	○	○	●
	2FMA-Netbank [101]	○	○	○	○	○	●	●	○
	SV-2FA [47]	●	●	●	●	○	●	○	●
	Device-aware 2FA [63]	●	●	●	○	○	●	○	●
Blink to Get In [52]	●	●	●	●	●	●	○	●	
Sajjad et al. [106]	●	●	●	●	●	●	○	●	
Automated Verification Schemes	Proximity-proof [54]	○	●	●	○	●	●	○	●
	Sound-proof [67]	○	●	●	○	●	●	○	●
	2FA-PP [125]	○	●	●	○	●	●	○	●
	Watermelon 2FA [90]	○	●	●	○	○	○	○	●
	SoundAuth [128]	○	●	●	○	●	●	○	●
	Luo et al [80]	○	●	●	○	●	●	○	●
	Wi-auth [110]	○	●	●	○	○	○	○	●
Listening Watch [113]	○	●	●	○	○	○	○	●	
T2FA [136]	○	●	●	○	○	○	○	●	
QuickAuth [137]	○	●	●	○	○	○	○	●	

● : Compliance ○ : Non-Compliance