COMPUTER SCIENCE & ENGINEERING
TEXAS A&M UNIVERSITY

SPIES
Security and Privacy in Emerging computing and networking Systems

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, Nitesh Saxena

Texas A&M University, College Station, TX, USA

usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Authentication mechanisms and types

- Verifies user identity before allowing access to online account.

Single-Factor Authentication (SFA)

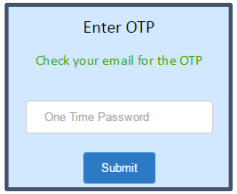
Two-Factor Authentication (2FA)

Multi-Factor Authentication (MFA)

Are these mechanisms secure?

- Cybercriminals are continuously introducing emerging attacks.
- To defend these attacks, researchers are introducing newer mechanisms.

Cybercriminal



Login Terminal Interaction

User Assisted Authentication

Automatic Authentication

Behavioural Authentication

Do these methods consider diverse users?

- Like screen reader-assisted users (e.g., blind users)?
- 2.2 billion people have vision related problem (1.2 billion incurable)
- They use online accounts for professional tasks across organizations.
- Access to blind users' accounts within an organization can expose sensitive organizational data and compromise whole organization.

Screen readers

World Health Organization

Data Breaches

Authentication schemes dedicated to screen reader assisted users

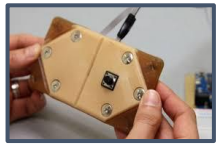
- Researchers developed authentication scheme dedicated for blind and visually impaired users.

Typing on Terminal

Gesture Based Authentication

Vibration Based Authentication

Behavioural Authentication



Special Hardware Based Authentication

Even if they are dedicated, are these schemes accessible and secure against emerging attacks targeting screen reader-assisted blind users?

Our contributions

Taxonomy and selection of authentication methods

We selected a total of 50 authentication methods of different types, consisting of 37 general-purpose methods and 13 methods specifically designed for visually impaired users.

A framework for security and accessibility assessment

The Authentication Literature Evaluation for Security and Accessibility (ALESA) framework comprises 5 accessibility and 8 security metrics to evaluate the security and accessibility of proposed methods.

Systematic evaluation of authentication proposals using codebook against metrics

We evaluated the selected authentication methods using a codebook to assess their adherence, non-adherence, or partial adherence to the framework's security and accessibility metrics.

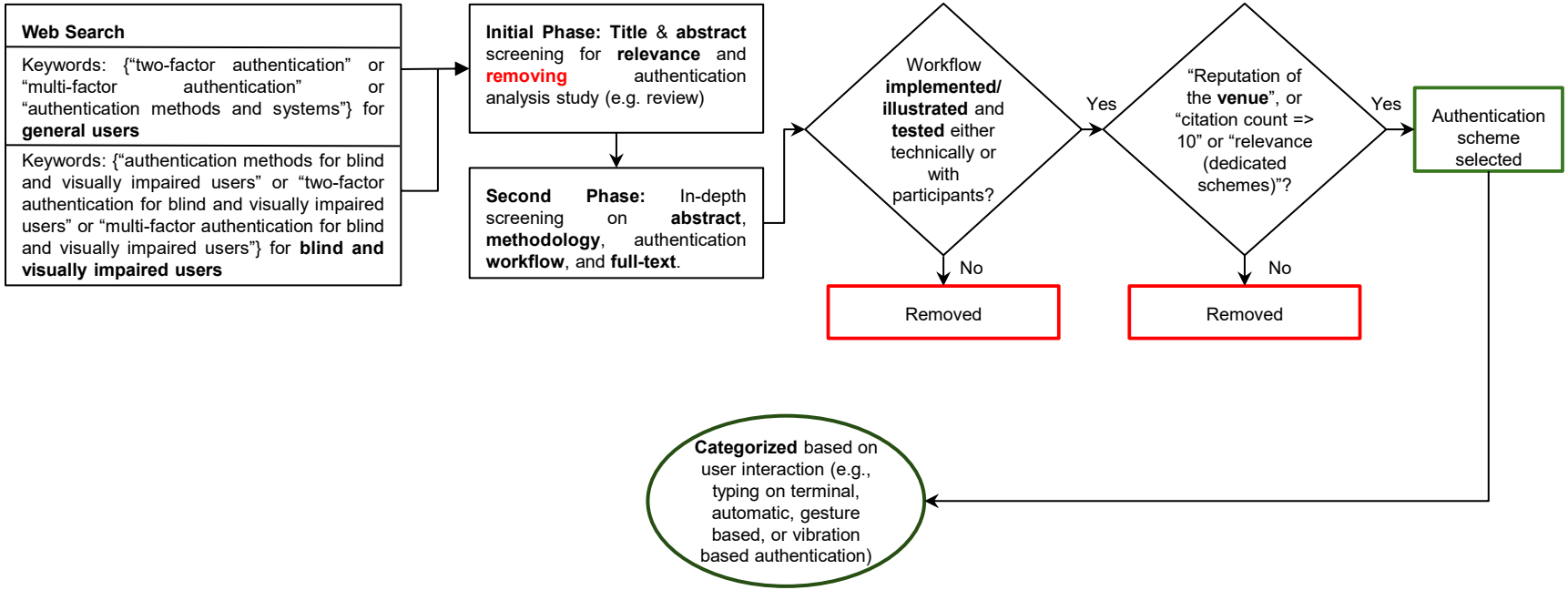
Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Selection of authentication methods

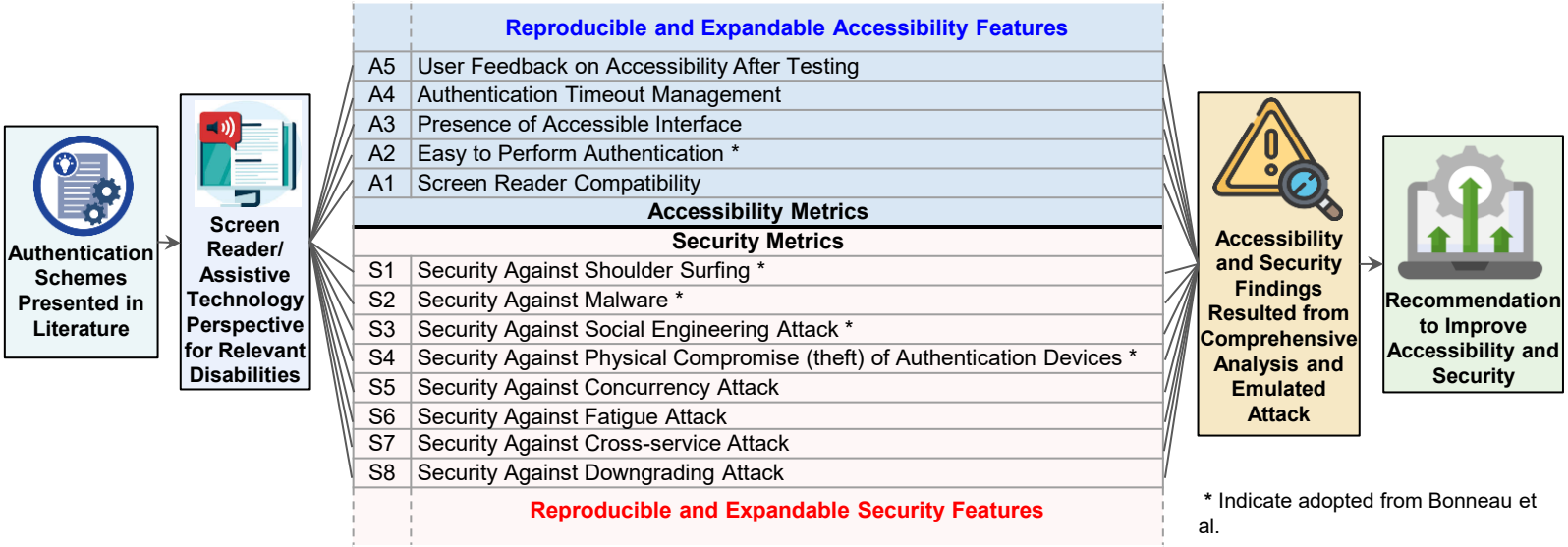


Process of selecting authentication methods

Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Selection and details of framework metrics

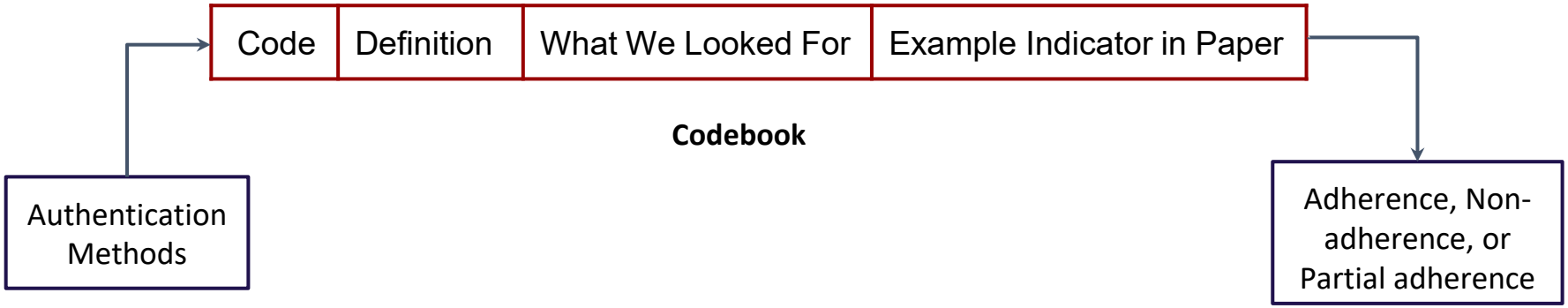


Overview of ALESA Framework

Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Application of framework metrics



Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Accessibility evaluation of general methods

Category	Login Terminal Interaction Schemes												User Assisted Verification Schemes															Automated Verification Schemes									
Authors Name	Chenchev [36]	Kaur [68]	Aloul et al. [10]	WebOTP [51]	Khan et al. [70]	Cheng [37]	TrustOTP [119]	TwoChain [97]	Mello et al. [104]	Papas pirou et al. [98]	Li et al. [75]	ALSaleem and Alshoshan [11]	DAMFA [93]	Mehrer 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]	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]
A1. Screen Reader Compatibility	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A2. Easy to Perform Authentication	○	○	○	◐	○	○	○	○	○	◐	○	◐	○	○	○	○	○	○	○	●	●	●	○	○	○	●	○	●	●	●	●	●	●	●	●	●	●
A3. Presence of Accessible Interface	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A4. Authentication Timeout Management	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	●	●
A5. User Feedback on Accessibility After Testing	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	○	○

* Adhere ●, not adhere ○, partially adhere ◐

General schemes demonstrate how they fail to meet the needs of diverse users.

Accessibility evaluation of general methods

Category	Login Terminal Interaction Schemes												User Assisted Verification Schemes														Automated Verification Schemes									
Authors Name	Chenchev [36]	Kaur [68]	Aloul et al. [10]	WebOTP [51]	Khan et al. [70]	Cheng [37]	TrustOTP [119]	TwoChain [97]	Mello et al. [104]	Papaspirou et al. [98]	Li et al. [75]	ALSaleem and Alshoshan [11]	DAMFA [93]	Mehrer 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]	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]
A1. Screen Reader Compatibility	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A2. Easy to Perform Authentication	○	○	○	◐	○	○	○	○	○	◐	○	◐	○	○	○	○	○	○	○	●	●	●	○	○	○	●	○	●	●	●	●	●	●	●	●	●	●
A3. Presence of Accessible Interface	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
A4. Authentication Timeout Management	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	●	●	●	●	●	●	●	●
A5. User Feedback on Accessibility After Testing	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	●	●	○	○	○	○	○	○	○

* Adhere ●, not adhere ○, partially adhere ◐

Automated schemes are easy to use and handle timeouts effectively, as they require little to no user interaction.

Security evaluation of general methods

Category	Login Terminal Interaction Schemes												User Assisted Verification Schemes															Automated Verification Schemes									
Authors Name	Chenchev [36]	Kaur [68]	Aloul et al. [10]	WebOTP [51]	Khan et al. [70]	Cheng [37]	TrustOTP [119]	TwoChain [97]	Mello et al. [104]	Papaspirou et al. [98]	Li et al. [75]	ALSaleem and Alshoshan [11]	DAMFA [93]	Mehrer 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]	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]
S1. Security Against Shoulder Surfing	○	○	○	○	○	○	●	●	◐	○	●	○	●	●	●	○	●	●	●	●	●	●	○	●	●	●	●	○	○	○	○	○	○	○	○	○	○
S2. Security Against Malware	○	○	○	○	○	○	●	●	○	○	●	●	●	●	●	●	●	○	○	○	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●
S3. Security Against Social Engineering Attack	○	○	○	●	○	○	●	○	○	○	○	○	●	●	●	●	●	○	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●
S4. Security Against Physical Compromise (theft) of Authentication Devices	○	○	○	○	○	○	○	○	○	○	●	○	●	○	○	○	●	○	○	○	○	○	○	●	○	●	●	○	○	○	○	○	○	○	○	○	○
S5. Security Against Concurrency Attack	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	○	○	○	●	●	●	●	○	○	●	●	●	●	●	●	●	●	●	●	●	●
S6. Security Against Fatigue Attack	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
S7. Security Against Cross-service Attack	○	○	○	○	○	○	●	○	○	○	●	○	○	●	●	○	●	○	●	●	●	●	●	○	○	○	○	○	○	○	○	○	○	○	○	○	○
S8. Security Against Downgrading Attack	○	○	○	●	○	○	●	○	○	○	○	○	●	●	●	●	●	○	●	●	●	●	○	●	●	●	●	●	●	●	●	●	●	●	●	●	●

* Adhere ●, not adhere ○, partially adhere ◐

Despite being inaccessible, it demonstrates resistance to many attacks, though some vulnerabilities still remain.

Accessibility evaluation of dedicated methods

Category	Typing on Terminal	Gesture Based Verification Schemes								Vibration Based Verification Schemes		Behaviour Based Scheme	Special Hardware Based Scheme
Authors Name	Longhua [77]	Banerjee and Hasan [20]	BlindLogin [58]	Balayogi and Kuppusamy [19]	Caporusso [32]	ARJUNA [18]	BraillePassword [9]	TouchIn [121]	VIBI [17]	Alsuhibany [12]	OneButtonPIN [66]	Haque et al. [55]	BendyPass [29]
A1. Screen Reader Compatibility	◐	○	●	○	●	●	●	○	●	○	●	○	○
A2. Easy to Perform Authentication	○	●	●	●	●	●	●	●	●	●	●	●	○
A3. Presence of Accessible Interface	○	○	●	○	●	●	●	●	●	○	●	○	○
A4. Authentication Timeout Management	○	○	○	○	○	○	○	○	●	●	●	●	○
A5. User Feedback on Accessibility After Testing	○	○	○	○	●	○	○	●	○	●	●	○	○

* Adhere ●, not adhere ○, partially adhere ◐

It shows comparatively better accessibility than general schemes but still lacks timeout handling and receives low user feedback ratings.

Security evaluation of dedicated methods

Category	Typing on Terminal	Gesture Based Verification Schemes								Vibration Based Verification Schemes		Behaviour Based Scheme	Special Hardware Based Scheme
Authors Name	Longhua [77]	Banerjee and Hasan [20]	BlindLogin [58]	Balayogi and Kuppusamy [19]	Caporusso [32]	ARJUNA [18]	BraillePassword [9]	TouchIn [121]	VIBI [17]	Alsuhibany [12]	OneButtonPIN [66]	Haque et al. [55]	BendyPass [29]
S1. Security Against Shoulder Surfing	○	○	○	○	●	○	○	●	●	●	●	●	○
S2. Security Against Malware	○	○	○	○	○	○	○	●	●	○	○	●	○
S3. Security Against Social Engineering Attack	○	○	○	○	●	○	○	●	●	○	○	●	○
S4. Security Against Physical Compromise (theft) of Authentication Devices	○	○	○	○	○	○	○	●	●	○	○	●	○
S5. Security Against Concurrency Attack	●	●	●	●	●	●	●	●	●	●	●	●	●
S6. Security Against Fatigue Attack	●	●	●	●	●	●	●	●	●	●	●	●	●
S7. Security Against Cross-service Attack	○	○	●	●	●	○	○	○	○	○	○	○	○
S8. Security Against Downgrading Attack	○	○	○	○	●	○	○	●	●	○	○	●	○

* Adhere ●, not adhere ○, partially adhere ◐

It is more accessible than general schemes but remains vulnerable to many attacks; however, some methods perform well.

Broader takeaways and lesson learned

Overlooked Diverse User Groups

Despite a broad user focus, general authentication schemes often overlook diverse user groups.

Automated Schemes Easy but Vulnerable

Automated schemes offer some accessibility (easiness and timeout management), but remain vulnerable to shoulder surfing, device theft, and concurrency attacks.

Dedicated but Does Not Meet Metrics

Schemes designed for blind users often claimed resistance to shoulder surfing, yet most remained vulnerable and lacked documented accessibility features, reflected in user study ratings, where only 4 out of 10 participants found them accessible.

Broader takeaways and lesson learned

Accessibility–Security Imbalance

Dedicated schemes (e.g., gesture- and vibration-based) offer better accessibility but weak security, while general schemes (user-assisted verification) provide stronger security but lack accessibility.

Authentication Risks Stemming from Screen Reader Use

Many vulnerabilities in these schemes arise from how users interact with authentication through screen readers.

Outline

- Selection of authentication methods
- ALESA Framework
  - Selection of framework metrics
  - Details of metrics
- Application of metrics on authentication methods
- Results
  - Accessibility and vulnerability Issues
  - Key takeaways
  - Insight for stakeholders
- Limitation, Potential Mitigation and Future Works

Limitation, Potential Mitigation, and Future Work

Limitation

- Although screen readers are also used by other diverse users (e.g., those with ADHD, dyslexia), we specifically designed the framework for blind users and did not consider other assistive technologies for them.
- However, we have noted how researchers or stakeholders can expand this framework to include other diverse users and test it with additional assistive technologies.

Mitigation

- Integrate AI and OS-level support to detect phishing, flag malicious links, and identify concurrent authentication prompts to mitigate accessibility-driven security risks.
- Use accessible on-screen drawing combined with behavioral traits (e.g., rhythm) and encrypt credentials with bidirectional validation between terminal and 2FA device to prevent observation, theft, and social engineering.

Future Work

- Future research should validate findings on expanding accessibility–security analysis to other user groups (e.g., cognitive or motor impairments) for a more inclusive framework.
- Future work should focus on integrating screen reader support, studying how updates affect blind users over time, and creating schemes that resist attacks while remaining fully navigable via assistive technologies.

Conclusion

- Current academic authentication schemes often fail blind and visually impaired users due to poor accessibility and security design.
- The ALESA framework exposes these gaps, urging future work on real-world validation and inclusive, secure authentication solutions.

Questions?


Thank
you!